iboss Secure Web Gateway

User Manual

SWOCA Delegated Administration

Note: Please refer to the User Manual online for the latest updates at www.iboss.com.

iboss Network Security makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defects. Further, this company reserves the right to revise this publication and make changes from time to time in the contents hereof without obligation to notify any person of such revision of changes.

www.iboss.com

Open Source Code

This product may include software code subject to the GNU General Public License (“GPL”), GNU Lesser General Public License (“LGPL”), or other open–source software licenses. Copies of the GPL and LGPL licenses are available upon request. You may also visit www.gnu.org to view more information regarding open–source licensing.

The GPL, LGPL and other open–source code used in iboss, Inc. products are distributed without any warranty and are subject to the copyrights of their authors. Upon request, open–source software source code is available from iboss, Inc. via electronic download or shipment on a physical storage medium at cost. For further details and information please visit www.iboss.com/.

4 INTERFACE

4.1 Dashboard

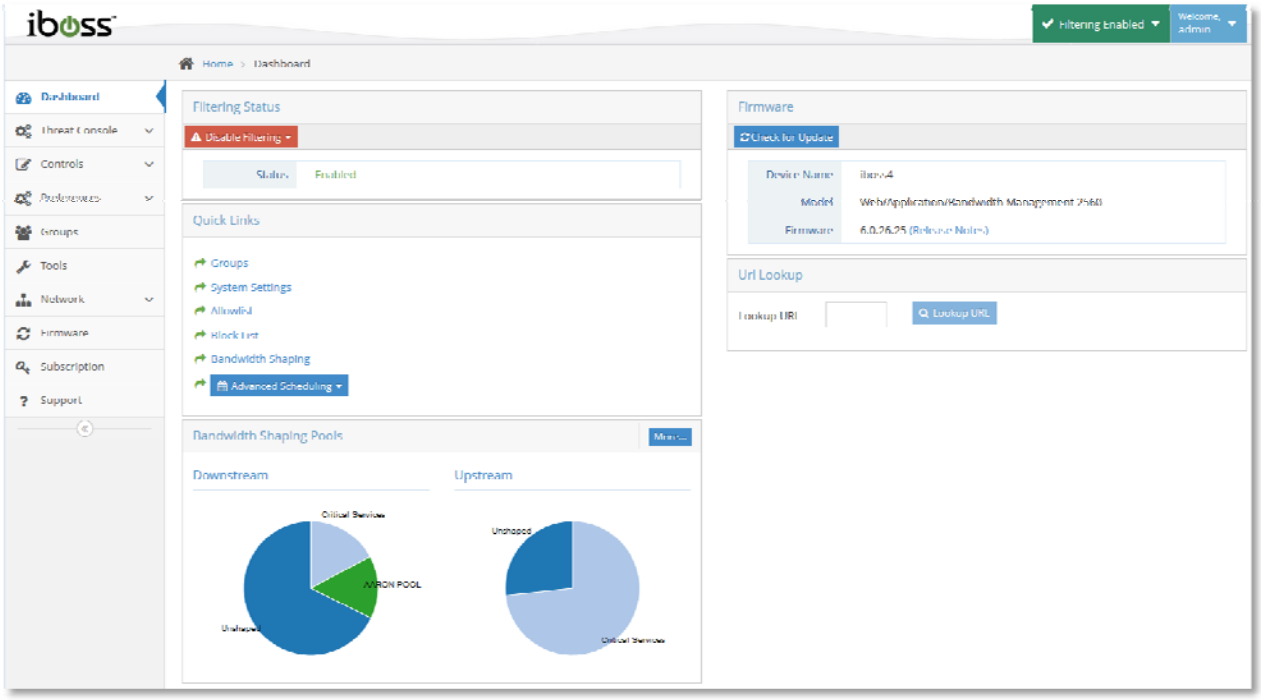


Figure 2 – Home Page

4.2 Widgets

4.2.1 Filtering Status

This indicates the filtering status of your iboss. The following values may be displayed:

Enabled – Indicates that your iboss is Enabled and Active.

Disabled – Indicates that your iboss is not enabled.

Connecting – When the iboss is enabled, it must first establish a connection to the gateway.

This indicates that the iboss is attempting to establish a connection.

Must Activate or Subscription Expired – If you have a new iboss and need to activate your subscription, or your iboss subscription has expired, the “Activate” button will appear next to the filtering status field. Click the “Activate” button to proceed with your iboss activation.

Current Date & Time – Indicates the current date and time. The date and time are synchronized when the iboss establishes a connection to the gateway, and are important for performing Internet scheduling and report logging. The local time zone settings may be set from the “Edit My Time Zone” page under “My Preferences”.

Note: The date & time will only be displayed when the iboss status is “Enabled”.

Enable/Disable Filtering Button – The “Enable/Disable” button is located above to the Filtering Status field. It is useful for quickly enabling and disabling your iboss filtering. If your status reads “Not Enabled”, clicking the “Enable” button will enable filtering. You may also choose to Disable for time periods such as 15 Min, 30 Min, 1 Hour, 2 Hours, 12 Hours, 24 Hours or Until Re–enabled.

4.2.2 Quick Links

This section provides links to common sections within the SWG interface.

4.2.3 Bandwidth Shaping Pools

This section provides a quick view of the current bandwidth pools.

4.2.4 Firmware

This section displays model and Firmware Version allowing for quick update actions.

4.2.5 URL Lookup

This section allows you to quickly lookup a URL on which categories it falls under.

4.3 Main Menu

The “**Home**” menu allows you to choose options for configuring the current iboss settings. These are options to choose from: **Dashboard, Threat Console, Controls, Preferences, Groups, Tools, Network, Firmware, Subscription,** and **Support.**

Dashboard – This option allows you to view status of the filtering and firmware version as well as quick links and tools that are most useful.

Threat Console – This option allows you to view your iboss report logs and configure settings for the Threat Console.

Controls – This section allows you to configure filtering policies for existing groups.

Preferences – This section allows you to edit preferences including E–mail options, Web GUI password, time zone and custom block messages.

Groups– This section allows you to identify computers and users on the network, as well as create filtering groups. This is also where you would create delegated administrators with the ability login to the iboss and access some or all portions of the User Interface.

Tools – This section is where to clear internal/DNS caches for the iboss and access the Backup & Restore menu. This is also where to trigger Filter–to–MDM synchronization if necessary.

Network – This section allows you to configure your iboss network settings.

Firmware – This section includes all firmware information for the iboss and allows you to update the firmware when updates are available.

Subscription –This page allows you to view your subscription status and add or update a Subscription Key.

Support – This page allows you to access information for support for the iboss SWG.

4.4 Top Shortcut Bar

Use the top right shortcut menu to Disable Filtering as well as changing the admin password and logging out.

7 Threat Console

This section allows you to configure how the SWG will log and report traffic flowing through it. You can configure the device to have onboard reporter to report to an external reporter.

7.1 Report Settings

7.1.1 General Settings

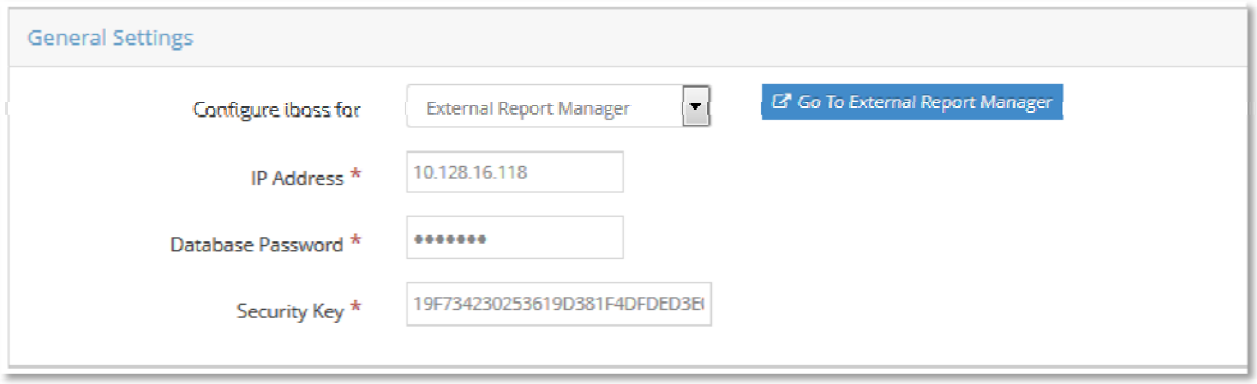


Figure 57 – Report Settings – General Settings

Configure iboss for – You may choose between Onboard Reporting and External Report Manager. If you have an External Report Manager, please choose External Report manager and refer to the following fields.

NOTE	This feature is only available with the Enterprise Reporter Appliance.

IP Address – Enter the IP address of the External Report Manager

Database Password – Enter the database password setup for the reporter. Default is ibossdb.

Security Key – Enter the security key from your reporter after adding it as a registered gateway.

7.1.2 Log Web Statistics

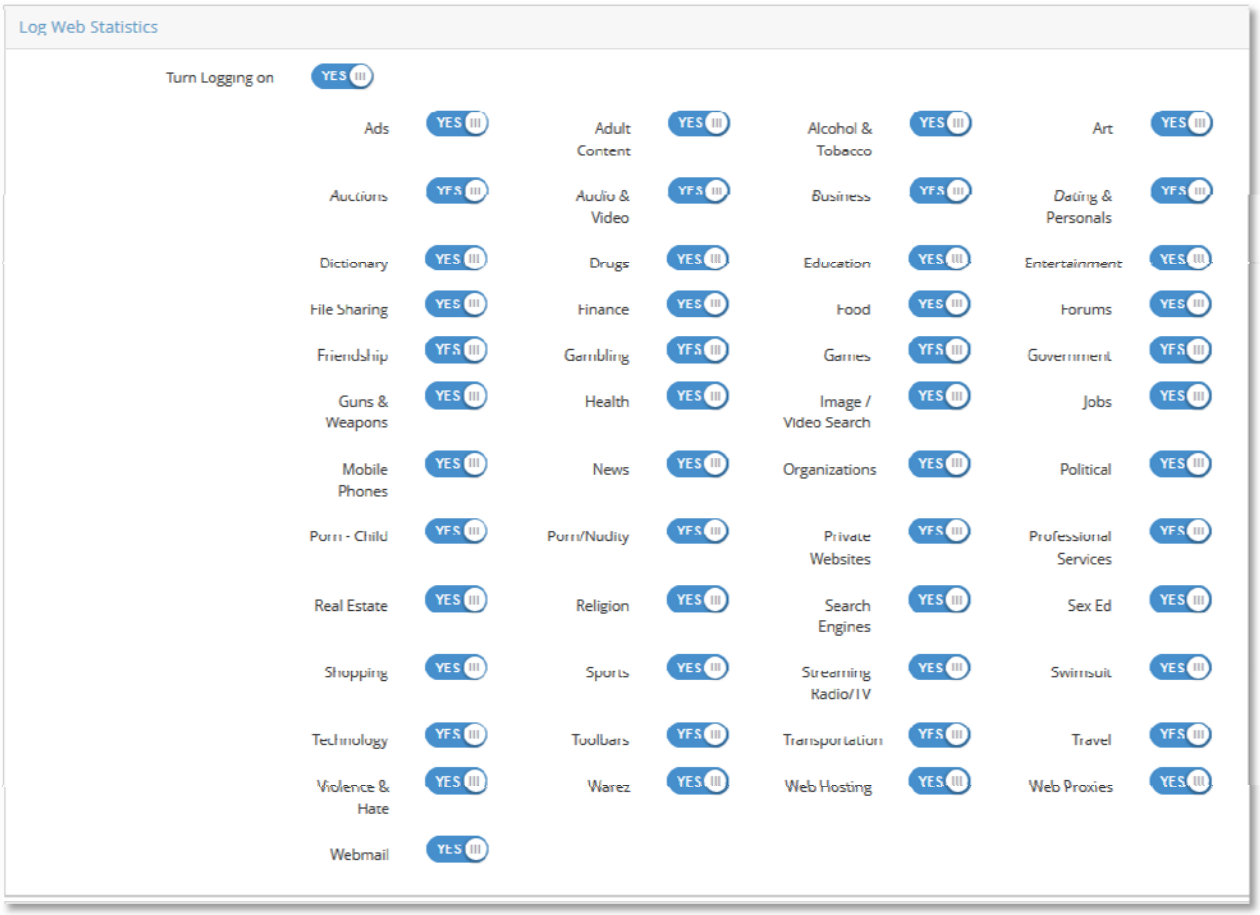


Figure 58 – Report Settings – Log Web Statistics

This allows you to enable or disable logging for web statistics. You may choose from the different categories to log.

7.1.3 Additional Settings

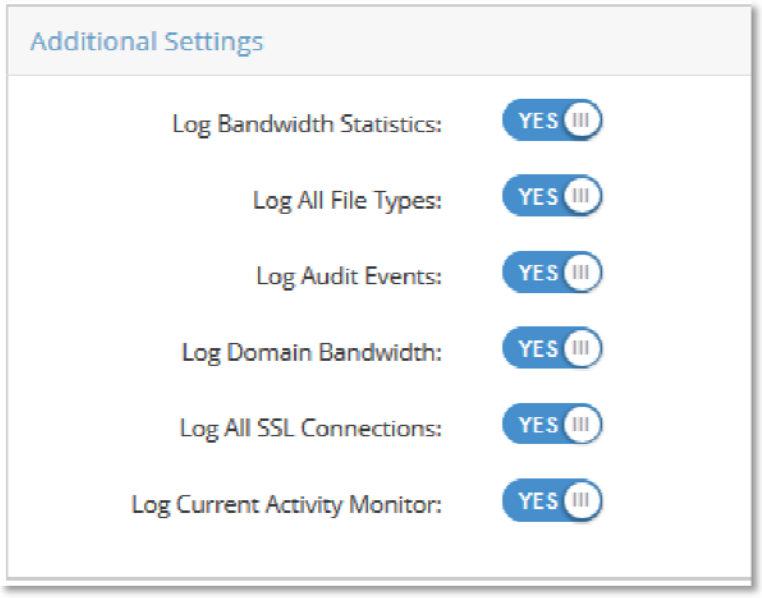


Figure 59 – Report Settings – Additional Settings

Log Bandwidth Statistics – This allows you to enable or disable logging bandwidth statistics.

Log All File Types – This allows you to enable or disable logging of all file types. By default, this is disabled for images, and resources on the page may not be logged in the URL Log.

Log Auditing Events – This allows you to enable or disable logging of auditing events. These are changes that are made in the controls of the iboss by delegated administrators. You can go to the Logs section of the reporter and change the "Audit Only" field to "Yes" allowing you to see all changes made to the configuration of the iboss, and by whom.

Log Domain Bandwidth – This allows you to enable or disable the logging of bandwidth per domain for statistics. This is disabled by default for faster performance.

Log All SSL Connections – This allows you to enable or disable logging for SSL connections.

Log Current Activity Monitory – This allows you to enable or disable the current activity monitor.

7.2 URL Pattern Ignore List

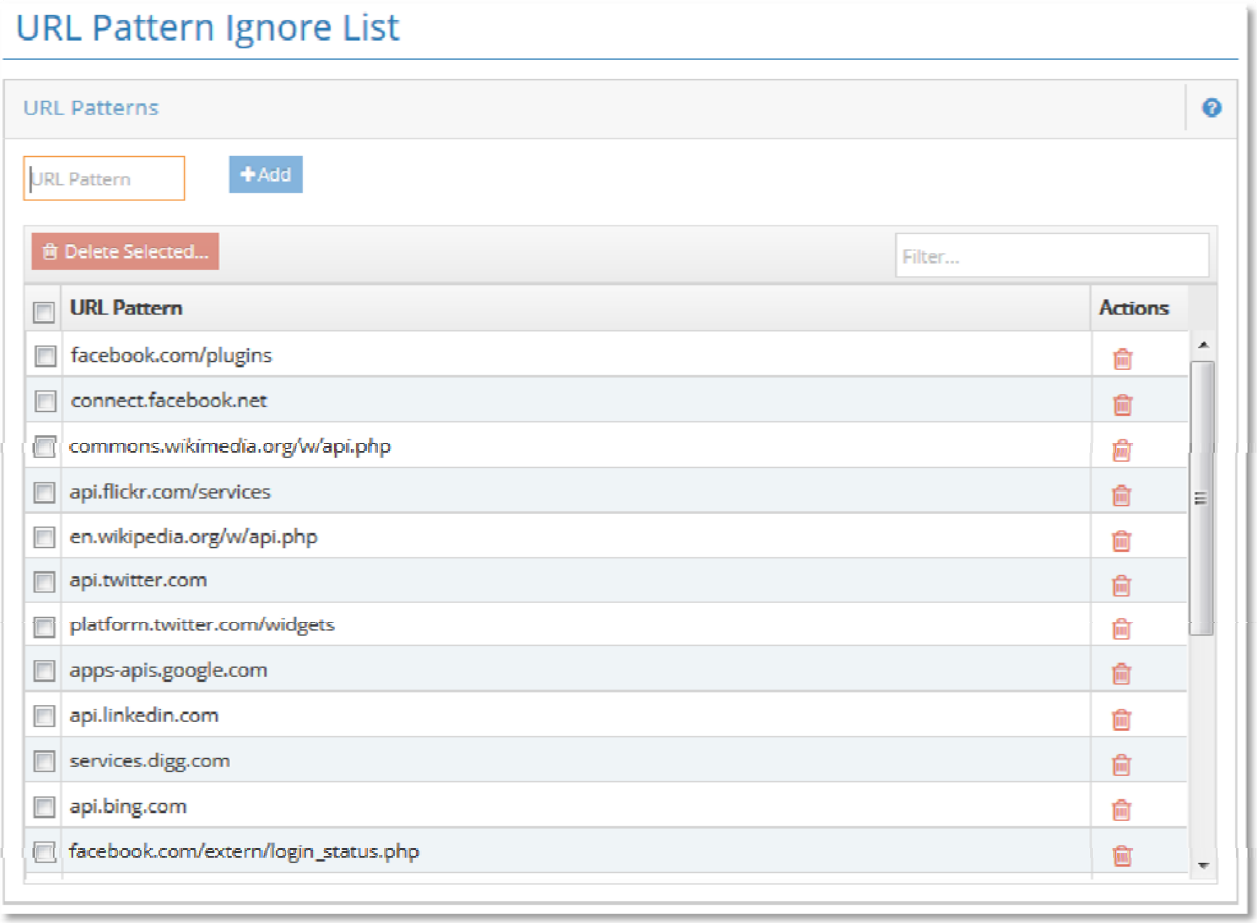


Figure 60 – Report Settings – URL Pattern Ignore List

This page allows you to add domains which you do not wish to log to the iboss Reports database. Domains in the list will be ignored from logging, however all filtering policies will still apply. This is useful for preventing the logging of sites like antivirus updates, operating system updates, etc.

Enter the domain or sub–domain of the website you would like to exclude from being logged to the iboss Reports database. Enter the domain in the text box below and click the "**Add**" button. To remove a website domain from the Ignore List, select the domain and click the "**Remove**" button located at the bottom of the page. When you are finished, click the "**Done**" button.

7.3 Reporter

This section brings you to the web interface of the Threat & Event Console. Please refer to the Threat Console Manual for more information.

8 Configure Controls

The "**Configure Controls**" menu lets you choose options for configuring the current iboss Internet controls.

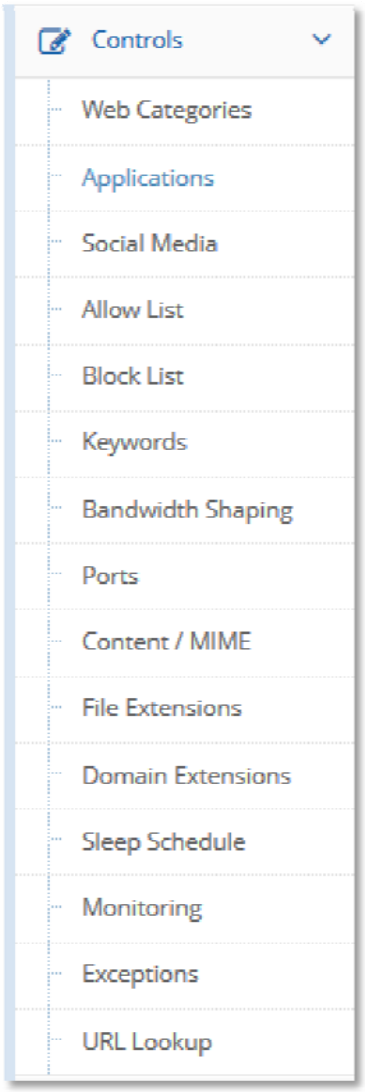


Figure 61 – Configure Internet Controls Menu

Web/SSL Categories – This section allows you to block or allow website content based on categories.

Applications Management – This section allows you to configure access to web applications that the iboss can manage. You may choose to block Chat (Instant messenger) programs, File Sharing programs, FTP & other protocols for Data Leakage Protection (DLP).

Advanced Social Media & Web 2.0 Controls – This section allows you to configure some of the social media sites and other web 2.0 sites like advanced Google and YouTube features. Another feature includes

Pinterest Controls. In addition, using the Local SSL Inspection Agent or Gateway SSL Decryption, other controls appear that can be used for social media sites such as Facebook, Twitter, and LinkedIn as well as more advanced Google controls.

Allow List – This section allows you to permit access to specific websites by adding them to the Allow List.

Block List – This section allows you to block access to specific websites by adding them to the Block List.

Keyword Blocklist / Allowlist – This section allows you to block specific keywords from searches or full URL's by adding them to the Keyword list.

Bandwidth Shaping – This section allows you to set bandwidth restrictions/limits & reservations on users, groups, domains, or web categories. Additional modules allow you to setup bandwidth pools for parent and child rules.

Port Blocking – This section allows you to block specific ports or port ranges with Protocol and Direction.

Content / MIME Type Restrictions – This section allows you to block specific content types and MIME types from being downloaded through the web.

File Extension Blocking – This section allows you to block specific file extensions from being downloaded on your network.

Domain Extension Restrictions – This section allows you to block or allow specific domain extensions from being accessed.

Sleep Schedule – This section allows you to schedule access to the Internet on a schedule.

Real–time Monitoring / Recording – This section allows you to set notification alerts for real–time monitoring and recording when thresholds are met.

Exception Requests – If enabled, a link on the block page will allow users to request the page be allowed. The requests are managed from this page.

URL Lookup – URLs can be searched here to determine how they are categorized. You can also submit a site for re–categorization.

8.1.1 Web / SSL Categories

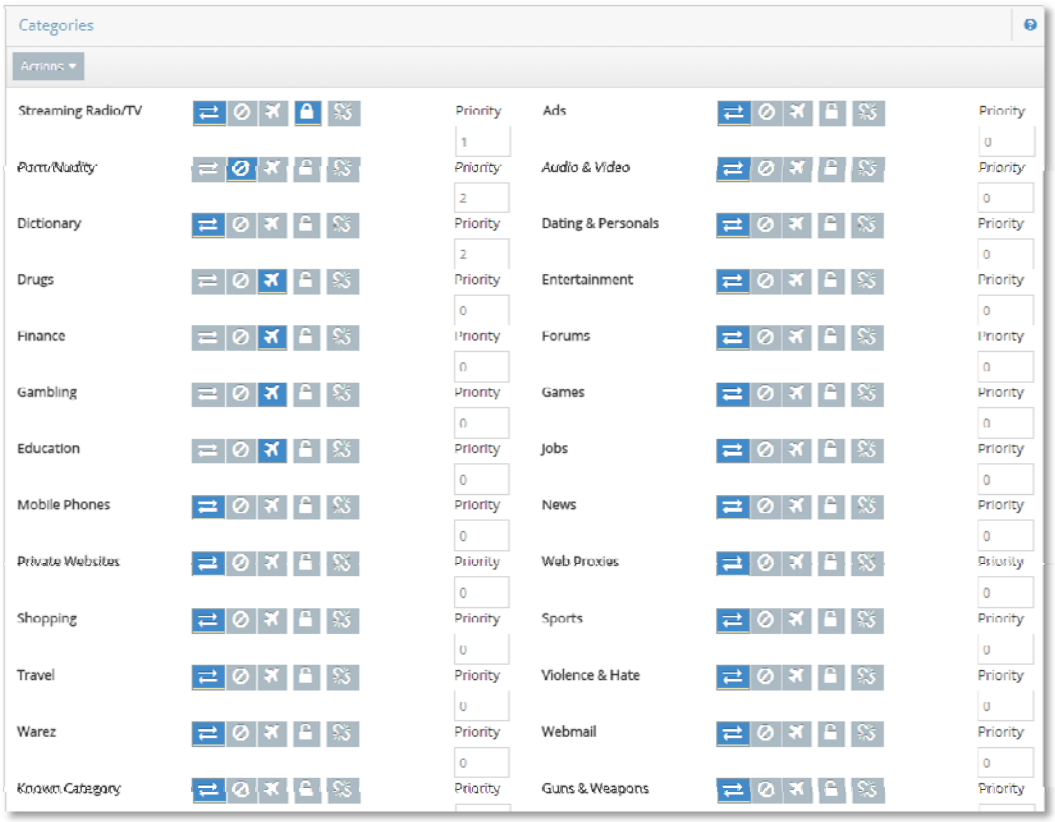


Figure 62 – Web/SSL Categories

The 'Web/SSL Categories' page allows you to configure the current iboss Internet website category blocking settings, log settings, Stealth Mode, and Identity Theft Detection options.

8.1.1.1 Category Scheduling

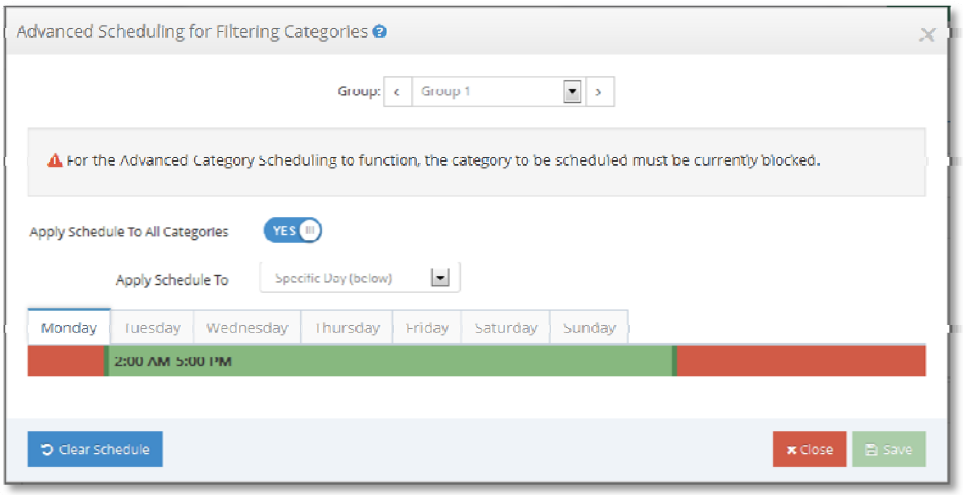


Figure 63 – Category Scheduling

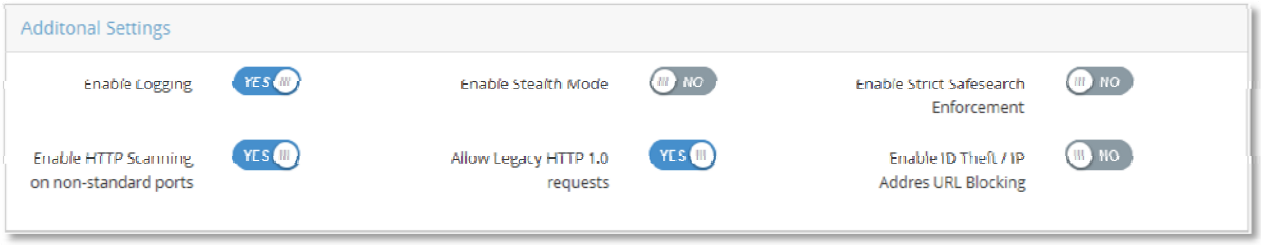
You may use advanced scheduling to create custom allow and block times for Filtering Categories. You may use different schedules for the different days of the week by selecting the day and setting the schedule. For Filtering Categories you will have to select a Category to Schedule:

Green (or checked) indicates access is allowed during the time block specified.

Red (or unchecked) indicates access is blocked during the time block specified.

Note: For the Advanced Category Scheduling to function, the category to be scheduled must be currently blocked on the "**Internet Category Blocking**" setup page.

8.1.1.2 Additional Settings



Enable Logging – Allows you to enable and disable logging of violation attempts for the current set of blocked website categories. Log reports may be viewed on the iboss Reports page. The report information includes date, time, user, website address, and category of the violation.

Enable Stealth Mode – Allows you to stealthily monitor Internet activity without blocking access to forbidden sites. With both Logging and Stealth Mode enabled, you can monitor Internet web surfing activity by viewing the log reports on the iboss Reports page while remaining unnoticed to Internet users on the network.

NOTE	Websites and online applications will not be blocked while the iboss is in "Stealth Mode."

NOTE	**Enable Strict SafeSearch Enforcement –** Allows you to enforce strict safe search preferences on Google, Yahoo, YouTube and Bing search engines. This includes image searching. If this option is enabled and the user does not have search engine preferences set to strict safe searching, the iboss will automatically change the user's preferences to strict safe searching before performing the search. This allows an extra layer of enforcement to prevent unwanted adult and explicit content from being searched for on these search engines.

Enable HTTP Scanning on Non–Standard Ports – If this feature is enabled, the iboss will scan for HTTP web requests on non–standard ports.

Allow Legacy HTTP 1.0 Requests – If this feature is enabled, the iboss will allow HTTP 1.0 requests that are missing the "HOST" header. Disabling this feature provides a higher level of filtering security and makes

bypassing the filter more difficult. If this feature is enabled, it may provide more compatibility with older non HTTP 1.1 compliant software.

Enable ID Theft / IP Address URL Blocking – Protects against potential identity theft attempts by notifying you when someone is trying to steal your personal information through Internet Phishing. Enabling this feature will also block users from navigating to websites using IP address URL's.

8.1.1.3 Categories

Figure 64 – Category Example

These are categories in which Internet websites are grouped. You may choose categories from this list that you wish to block on your network. In addition to blocking access to these website categories, the iboss will also log attempted access violations if logging is enabled.

Examples of website categories are:

Ads	**Forums**	**Private Websites**
Adult Content	**Friendship**	**Real Estate**
Alcohol/Tobacco	**Gambling**	**Religion**
Art	**Games**	**Restaurants/Food**
Auctions	**Government**	**Search Engines**
Audio & Video	**Guns & Weapons**	**Services**
Bikini/Swimsuit	**Health**	**Sex Ed**
Business	**Image/Video Search**	**Shopping**
Dating & Personals	**Jobs**	**Sports**
Dictionary	**Mobile Phones**	**Streaming Radio/TV**
Drugs	**News**	**Technology**
Education	**Organizations**	**Toolbars**
Entertainment	**Political**	**Transportation**
File Sharing	**Porn/Nudity**	**Travel**
Finance & Investment	**Porn – Child**	**Violence & Hate**

Virus & Malware **Web Hosting**

Web–Based E–mail **Web Proxies**

Allow/Block/Stealth – Specifies whether the category is blocked or allowed for this filtering group. Designating 'Stealth' will flag as a violation but will not actually block.

Priority – By default 'Block' has priority over 'Allow'. A site belonging to multiple categories will be blocked if ANY of those categories are blocked unless a category with a higher priority is allowed. For example: A site belonging to both 'Education' and 'gaming' would be blocked if the policy is to block all gaming. If 'Education' priority is bumped to 1 (or anything higher than that of gaming) then the site is allowed.

Locked – A Delegated Administrator will not be able to alter the category settings of those flagged as 'Locked'.

No Override – A Delegated Administrator will not be able to add URLs to the Allow list if they belong to a banned category marked as 'No Override'.

8.1.1.4 Identify Theft (Phishing)/ IP Address Blocking Page

When a page is blocked from of the iboss due to detection of Identity Theft (Phishing)/IP

Address URL Blocking, this page will show up in the web browser to the user. You may manually login and add the blocked Identity theft page (IP address) to the allow list if you feel that you have received the Identity Theft Detection in error by typing in the password and pressing Login.

8.1.2 Application Management

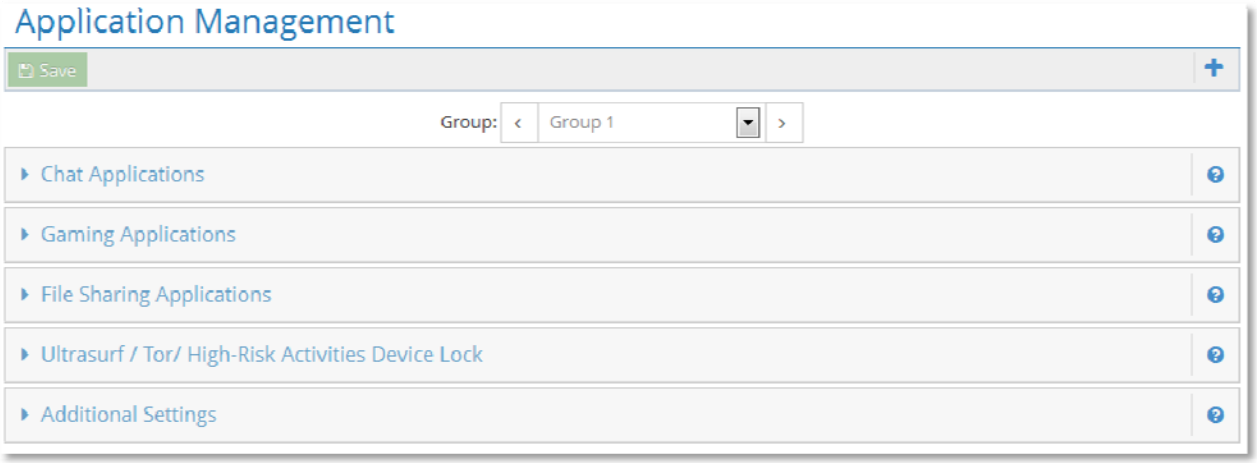


Figure 65 – Application Management

The "Application Management" section allows you to configure the current iboss program blocking settings.

8.1.2.1 Chat Applications

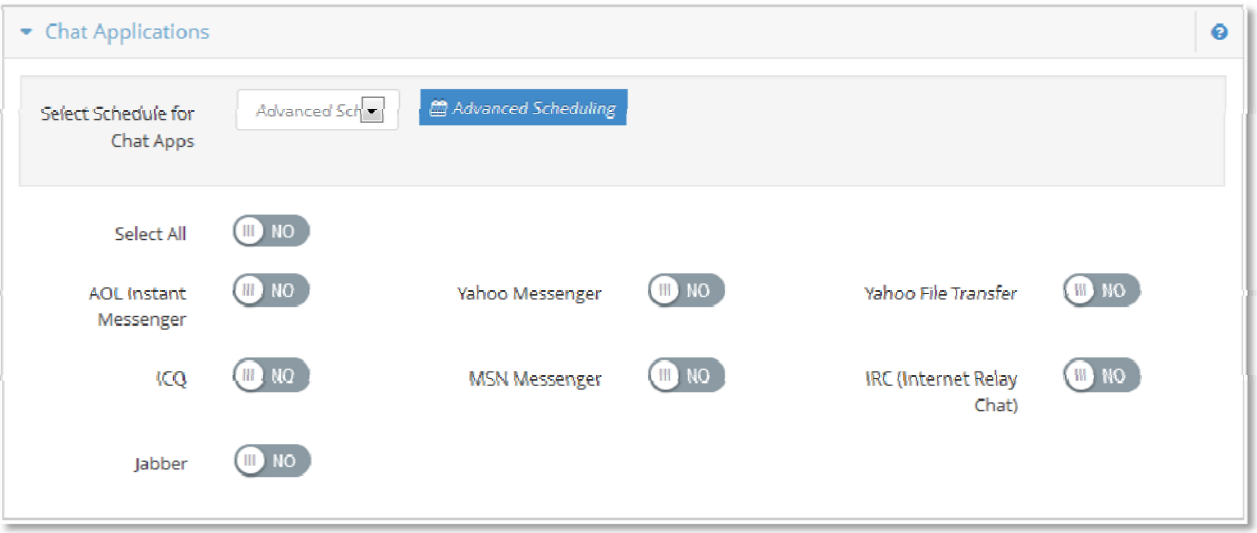


Figure 66 – Applications – Chat Applications

This category contains applications used for online messaging and chat. The iboss can block the selected program(s) and log attempted violations. Examples of applications in this category are:

AIM (AOL Instant Messenger)

Yahoo Messenger/Yahoo File Transfer

ICQ

MSN Messenger

IRC (Internet Relay Chat)

Jabber

Advanced Scheduling – Allows you to schedule daily access for selected chat programs. This option will bypass blocking for chat and instant messenger programs during the specified time.

8.1.2.2 Gaming Applications

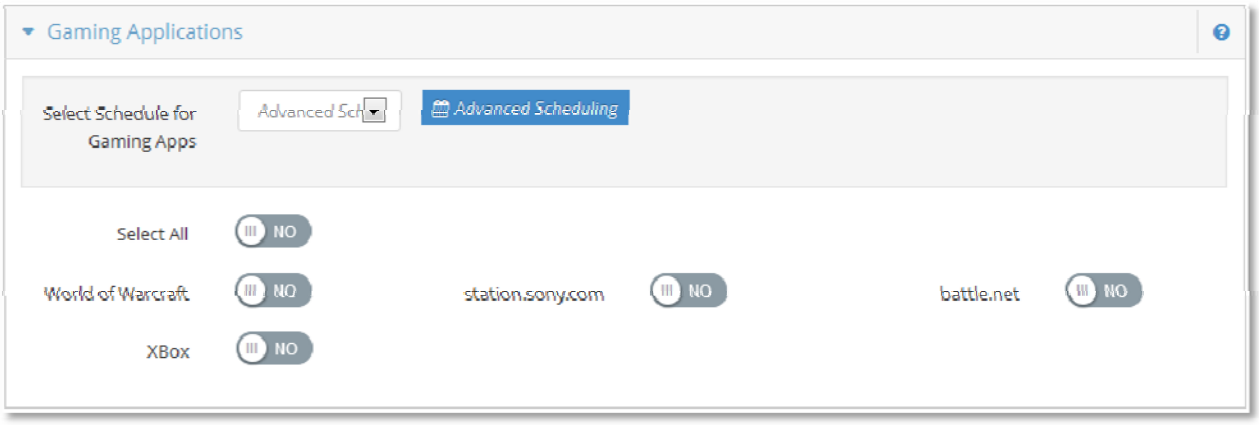


Figure 67 – Applications – Gaming Applications

This category contains online gaming applications. The iboss can block the selected program(s) and log attempted access violations. Examples of applications in this category are:

World of Warcraft

StarCraft

Station.sony.com

Battle.net

XBox

Advanced Schedule – Allows you to schedule daily access for selected online gaming programs. This option will bypass blocking for online gaming programs during the specified time.

8.1.2.3 File Sharing Applications

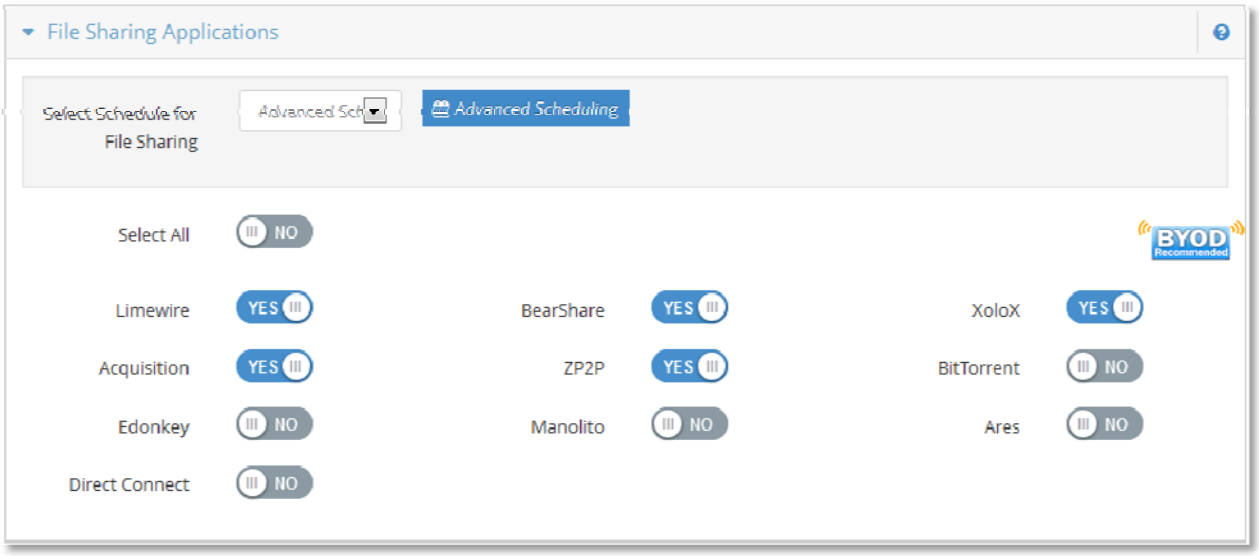


Figure 68 – Applications – File Sharing Applications

This category contains online file sharing applications. The iboss can block the selected program(s) and log attempted access violations. Examples of applications in this category are:

LimeWire	**Acquisition**	**Ares**
XoloX	**BitTorrent**	**Direct Connect**
ZP2P	**Edonkey**	
BearShare	**Manolito**	

Advanced Scheduling – Allows you to schedule daily access for selected file sharing programs. This option will bypass blocking for file sharing programs during the specified time.

8.1.2.4 Ultrasurf / Tor / High–Risk Activity Device Lock

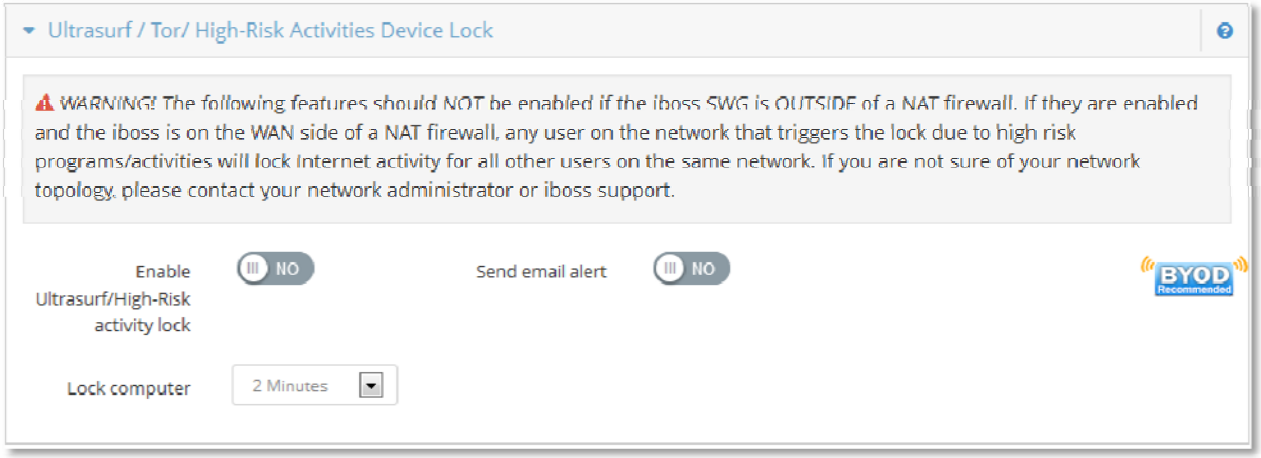


Figure 69 – Ultrasurf / Tor / High–Risk Activity Device Lock

Enable Ultrasurf/High–Risk activity lock – This feature blocks the use of Hotspot Shield, OpenVPN, Spotflux, and Expat Shield. It also allows you to lock the Internet for a user if the use of Ultrasurf/Tor Proxies is detected. This blocks all Internet access so that when the user opens a web browser, they will be informed that the detection has occurred and that they must disable the program. The Internet will be blocked for the specified time.

Send email alert – This option will inform the iboss administrator that the detection has occurred when the event is detected. By default, it will email the address setup for the User Alerts (Reporter → Registered Devices). The individual filtering group can have a group email contact under Controls → Monitoring. The email address listed in the Monitoring section, for any given group, will override the master alerts email address listed in the Reporter.

Lock computer – When Ultrasurf/high–risk activity is detected allows you to specify an amount of time in minutes that the user would be locked for. This will lock the computer from going to the Internet from the time it has detected this event for the amount of minutes that you specify. The suggested setting for this value is 5 minutes, but you can set a lower or higher value.

You can unlock a computer manually by finding the computer under the Groups→ Computers tab and click Unlock.

WARNING! These features should NOT be enabled if the iboss SWG is OUTSIDE of a NAT firewall. If they are enabled and the iboss is on the WAN side of a NAT firewall, any user on the network that triggers the lock due to high risk programs/activities will lock Internet activity for all other users on the same network. If you are not sure of your network topology, please contact your network administrator or iboss support.

8.1.2.5 Additional Settings

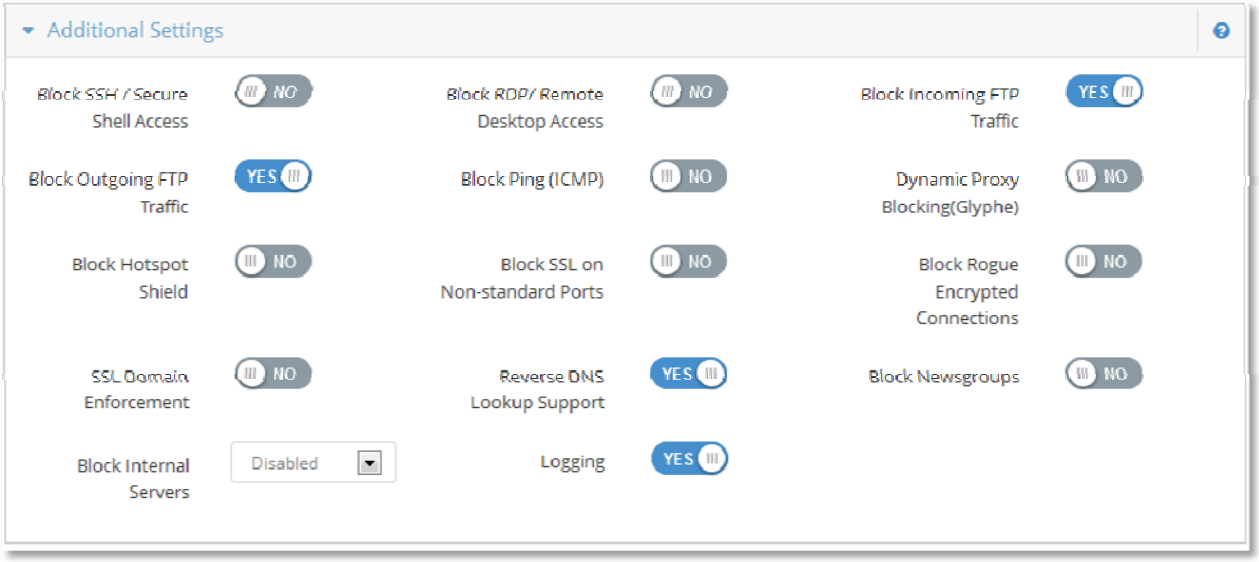


Figure 70 – Application – Additional Settings

Block SSH/Secure Shell Access – You may choose block incoming and outgoing SSH Shell Access.

Block RDP/Remote Desktop Access – You may choose to block incoming and outgoing Remote Desktop Access.

Block Incoming FTP Traffic – You may choose to block incoming FTP Traffic.

Block Outgoing FTP Traffic – You may choose to block outgoing FTP Traffic.

Block Ping (ICMP) – You may choose to block outgoing Ping (ICMP) Traffic.

Dynamic Proxy Blocking (Glype) – You may choose to block dynamic Glype–themed proxy sites. These are proxy sites setup using the Glype Proxy script which the iboss can detect and block dynamically regardless of the domain.

Block Hotspot Shield – You may choose to block Hot Spot Shield. Hot Spot Shield is a program used to proxy to Hot Spot Shields servers. Enabling this feature will block the program from being used as a proxy.

Block SSL on Non–Standard Ports – You may choose to enable blocking SSL on Non–Standard Ports. This feature is useful for blocking File Sharing programs which use encryption over non–standard ports.

Block Rogue Encrypted Connections – You may choose to enable blocking for Rogue Encrypted Connections. This option blocks invalid SSL certificates and blocks programs that use Rogue Encryptions such as UltraSurf.

SSL Domain Enforcement – This option validates domains with the SSL certificate.

Reverse DNS Lookup Support – This option allows for Reverse DNS lookup support, tracing an IP back to the domain it belongs to.

Block Newsgroups – You may choose to block newsgroup traffic.

Block Internal Servers – You may choose to enable blocking for internal Servers. This option helps block programs like BitTorrent which upload as well as download.

Logging – Allows you to enable or disable logging of attempted program access violations. This log is found on the Reports page. The logging includes date, time, and category. Logging can be enabled while in stealth mode. This is useful for monitoring your Internet usage while remaining unnoticed on the network. Without logging, the iboss program blocking will still work however violations will not be logged.

8.1.3 Advanced Social Media & Web 2.0 Controls

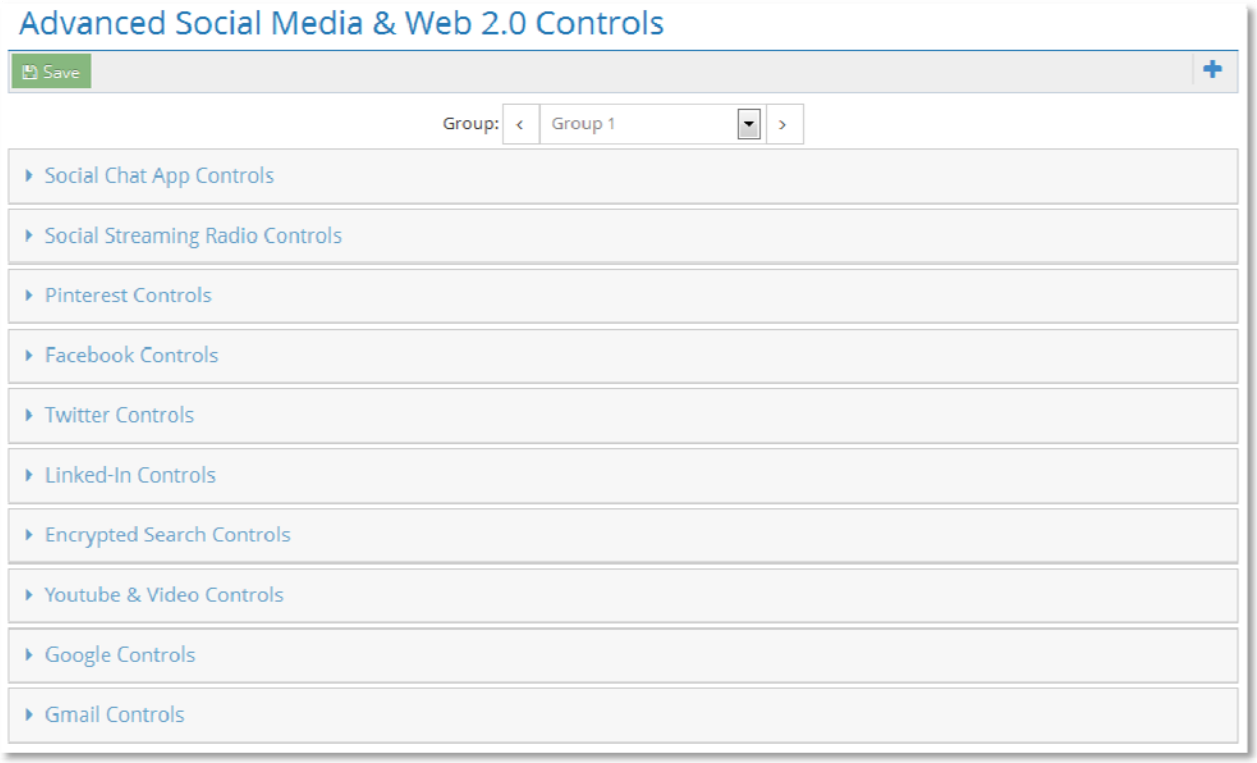


Figure 71 – Advanced Social Media & Web 2.0 Controls

8.1.3.1 Social Chat App Controls

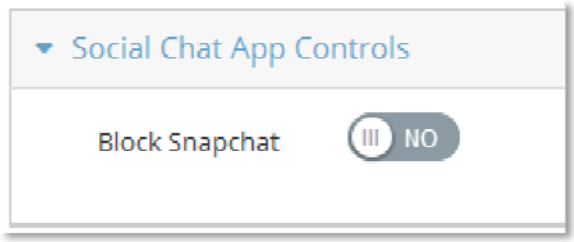


Figure 72 – Social Chat App Controls

This feature allows you to block the Snapchat application on mobile devices.

8.1.3.2 Social Streaming Radio Controls

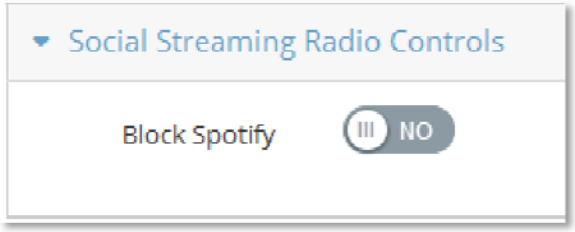


Figure 73 – Social Streaming Radio Controls

This feature allows you to block Spotify.

8.1.3.3 Pinterest Controls

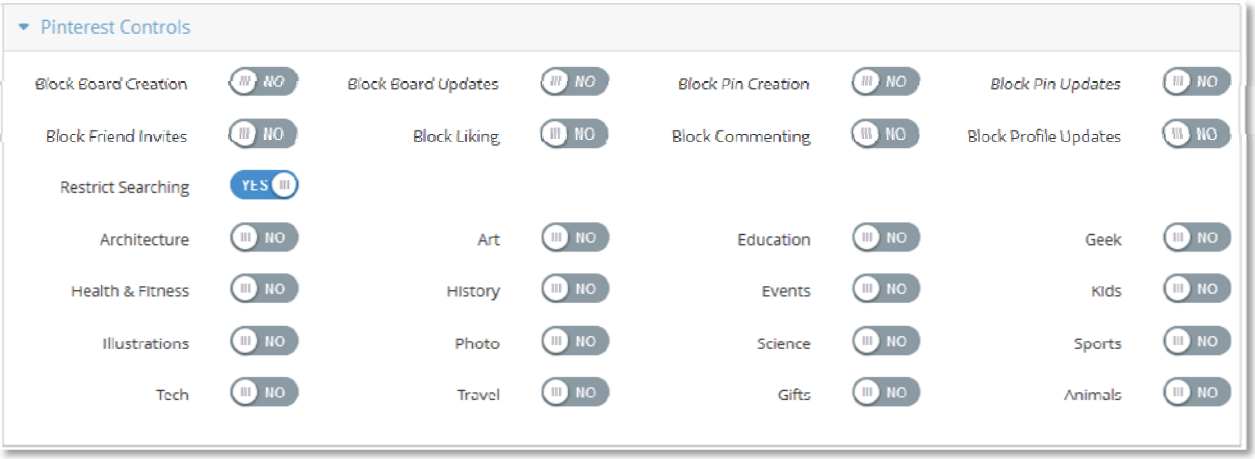


Figure 74 – Pinterest Controls

These features allow you configure particular sections of Pinterest websites. The following options are available to choose to block:

- Block Board Creation
- Block Board Updates
- Block Pin Creation
- Block Pin Updates
- Block Friend Invites
- Block Liking
- Block Commenting
- Block Profile Updates

- Restrict Searching to selected categories:
  - Architecture
  - Art
  - Education
  - Geek
  - Health & Fitness
  - History
  - Events
  - Kids
  - Illustrations
  - Photo
  - Science
  - Sports
  - Tech
  - Travel Gifts
  - Animals

8.1.3.4 Facebook Controls

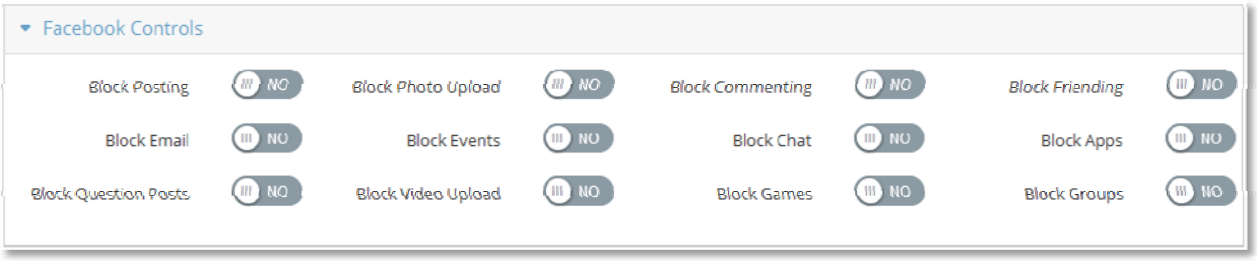


Figure 75 – Facebook Controls

SSL Decryption for facebook.com needed – These features allow you to block specific features and sections for facebook.com. The following options are available to choose to block:

- Block Posting
- Block Photo Upload
- Block Commenting
- Block Friending
- Block Email
- Block Events
- Block Chat
- Block Apps
- Block Question Posts
- Block Video Upload
- Block Games
- Block Groups

8.1.3.5 Twitter Controls

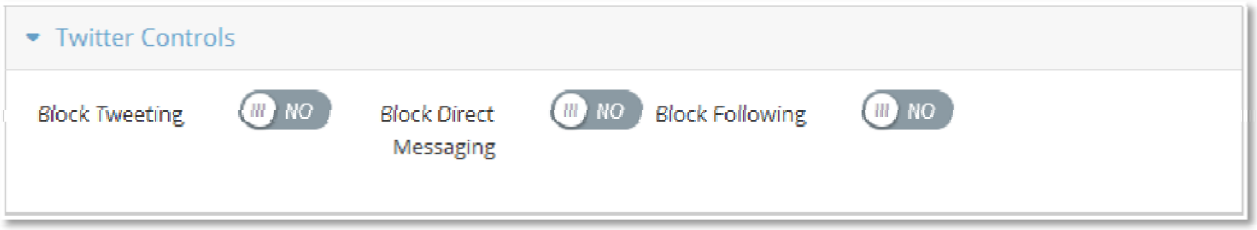


Figure 76 – Twitter Controls

SSL Decryption for twitter.com needed – These features allow you to block specific features and sections for twitter.com. The following options are available to choose to block:

- Block Tweeting
- Block Direct Messaging
- Block Following

8.1.3.6 Linked–in Controls

Figure 77 – Linked–in Controls

SSL Inspection Agent needed – These features allow you to block specific features and sections for linkedin.com. The following options are available to choose to block:

- Block Posting/Profile Edit
- Block Mail
- Block Connections
- Block Job Search

8.1.3.7 Encrypted Search Controls

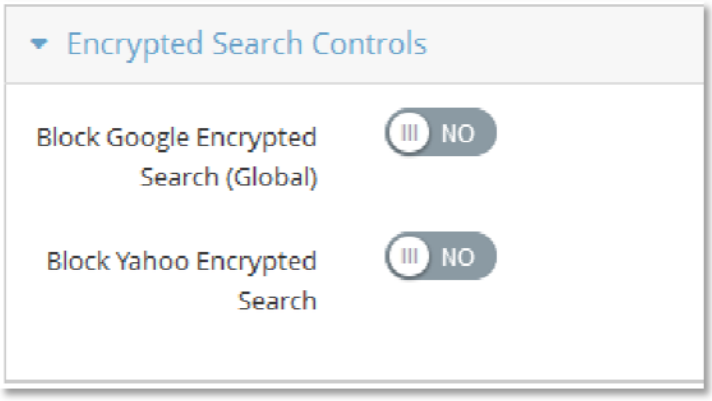


Figure 78 – Encrypted Search Controls

Block Google Encrypted Search (Global) – Allows for automatic redirections to unencrypted search pages.

Block Yahoo Encrypted Search – Allows for blocking of Encrypted Yahoo Searches. HTTP requests for yahoo.com get directed to an non–encrypted search page.

8.1.3.8 YouTube & Video Controls

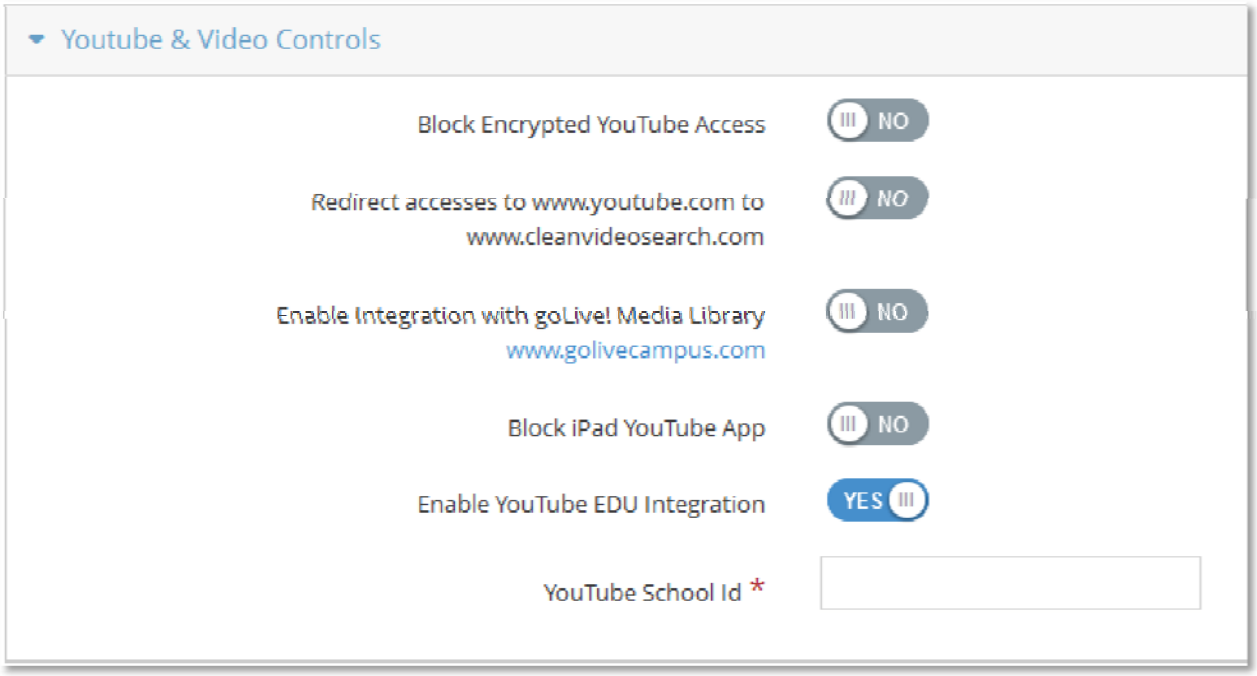


Figure 79 – YouTube & Video Controls

These features allow you to controls certain features of YouTube as well as handle requests to YouTube differently for specific filtering groups.

Block Encrypted YouTube Access – This option will block encrypted https access to YouTube (now on a per–group basis). If your DNS server has direct access to the Internet without going to through the iboss or you have

the iboss in tap mode, you would want to setup a DNS Conditional Forwarder for youtube.com to point to the iboss. You can get these instructions from iboss support.

Redirect accesses to www.youtube.com to www.cleanvideosearch.com – This redirects any request to youtube.com to cleanvideosearch.com. Cleanvideosearch.com is a site that provides searching for videos from YouTube.com while enforcing Strict Safety Mode and stripping out all comments and related videos. You can set this option on a per group basis.

Enable Integration with goLive! Media Library www.golivecampus.com – This feature allows you to block YouTube.com but allow videos to be played from golivecampus.com. Golivecampus.com is a site that allows you to granularly choose which videos are allowed to be viewed with channels that can have videos linked on them.

Block iPad YouTube App – This option allows you to block the YouTube App on mobile devices.

Enable YouTube EDU integration – This feature integrates with YouTube for Schools. This allows you to enter your **YouTube School ID** and this will be appended to each request to YouTube allowing only educational videos from YouTube to be allowed to play.

8.1.3.9 Google Controls

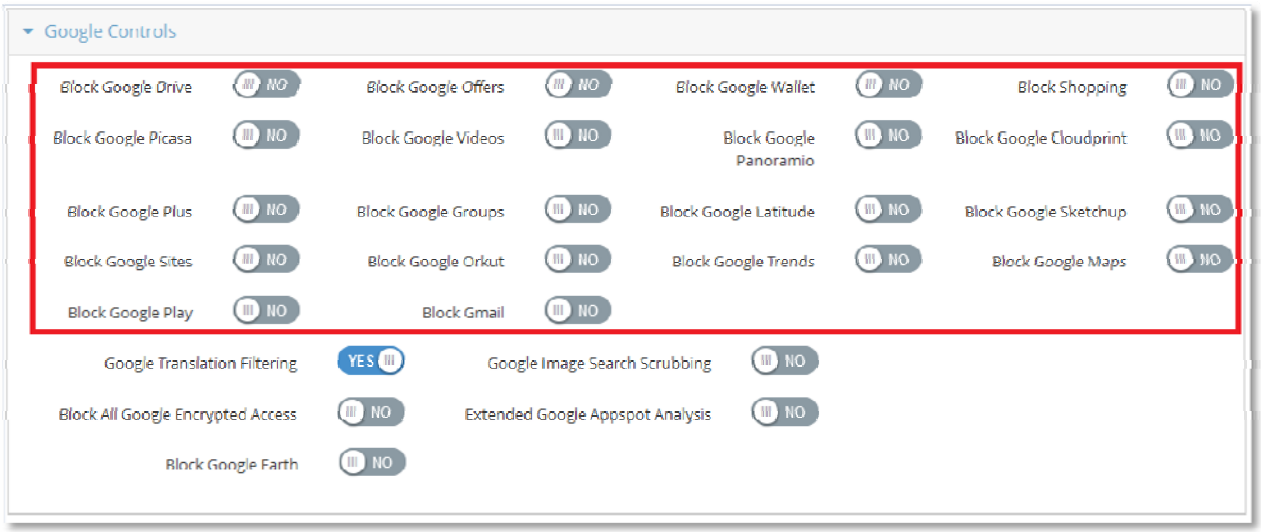


Figure 80 – Google Controls

Features in the red box above need SSL Decryption – These features from Google in allow you to control specific sections of Google by decrypting and enabling these features.

Google features that are available when enabling the SSL inspection Agent/Enabling Gateway Decryption are:

- Block Google Drive
- Block Google Offers
- Block Google Wallet
- Block Shopping
- Block Google Groups
- Block Google Latitude
- Block Google SketchUp
- Block Google Sites
- Block Google Orkut
- Block Google Trends
- Block Google Maps

- Block Google Picasa
- Block Google Videos
- Block Google Panoramio
- Block Google Cloudprint
- Block Google Plus

Google Translation Filtering – This feature blocks violation sites from being translated using Google Translation.

Google Image Search Scrubbing – This feature strips out images on Google Image Searches that come from violation sites that are block by the categories.

Block All Google Encrypted Access – This feature blocks all encrypted Google services.

Extended Google Appspot Analysis – This feature lets you allow access to appspot.com but block subdomains of appspot.com based on DNS.

Block Google Earth – This feature blocks Google Earth.

8.1.3.10 Gmail Controls

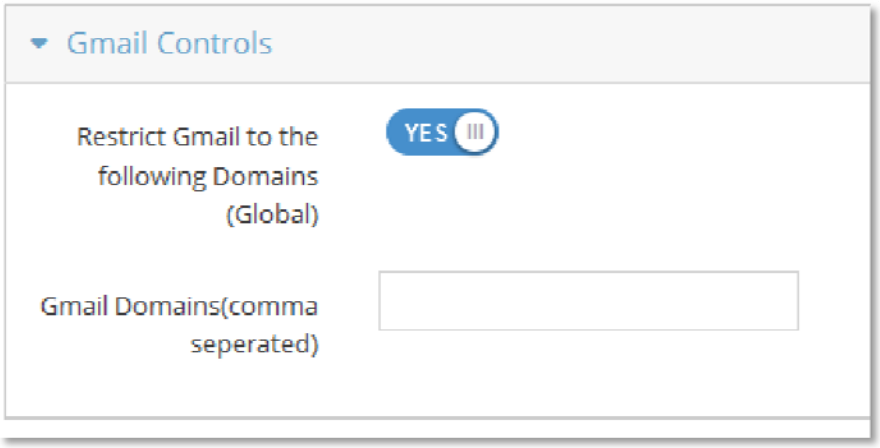


Figure 81 – Gmail Controls

Restrict Gmail to the following Domains (Global) – This features allows you to restrict Gmail access to only the domains you specify.

8.1.4 Allowlist

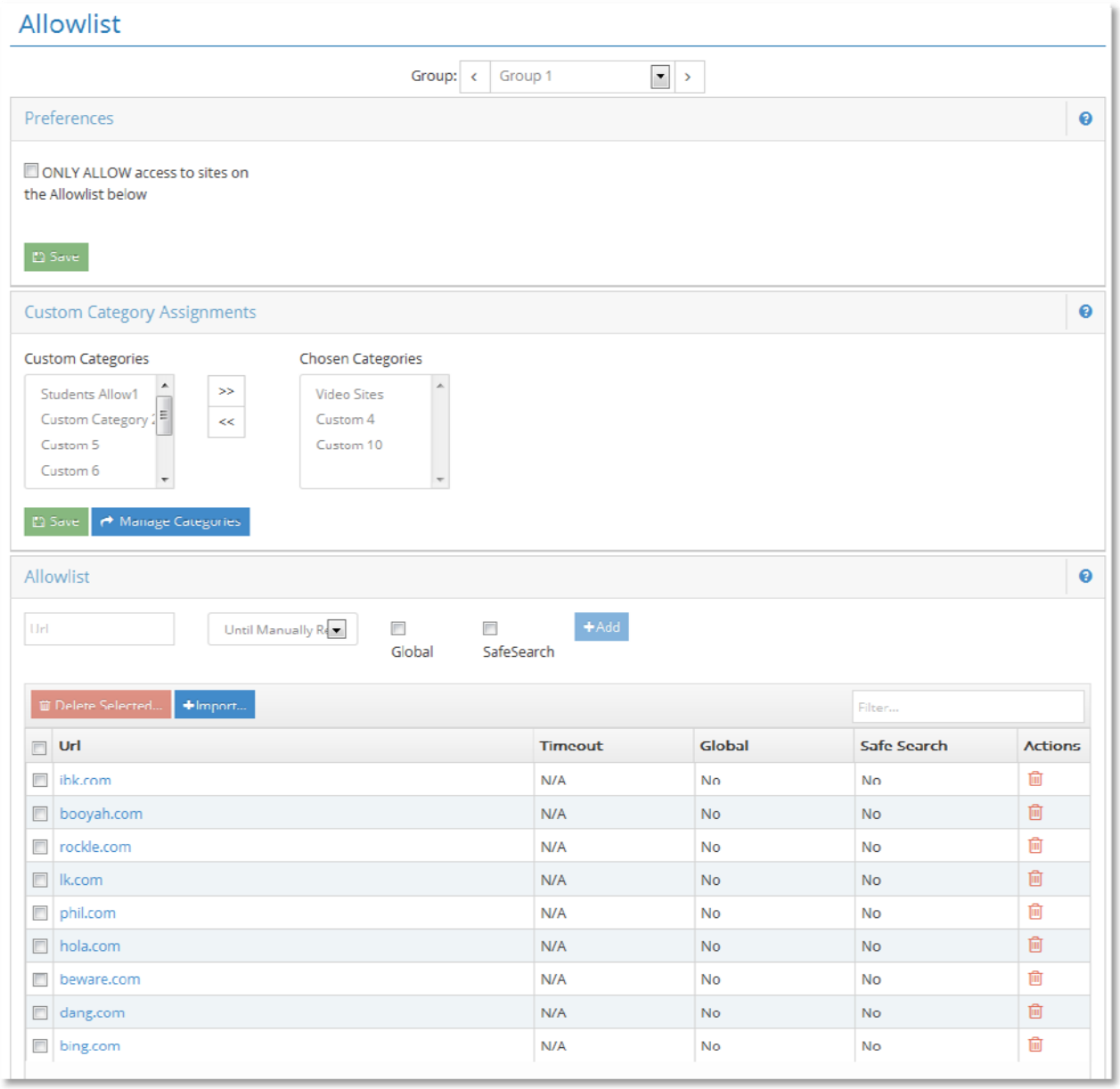


Figure 82 – Allowlist

This page allows you to add specific websites to your Allow list. The Allow list is a list of specific Internet URLs that you want to allow on your network. Website URLs added to this list will be allowed even if they are currently blocked in the Web Categories section.

8.1.4.1 Preferences

Allow ONLY access to sites on the Allow list – Checking this option will **only** allow sites on the list.

Alert! If the "**Allow ONLY access to sites on the Allow list**" option is selected, only the websites in the Allow list below will be allowed. All other websites will be blocked.

Enable Allow list Navigation webpage – This will give you a page that has a list of the allowed sites to be able to give to your users. You may select the "**Enable Allow list Navigation webpage**" if you wish to allow access to a built–in iboss website that will display links to all sites on the Allow list. To apply changes, click the "**Apply**" button.

Note: The Allow list Navigation webpage will only display when the "**Allow ONLY**" feature is enabled.

Default Timed URL Timeout – This is the default setting for when adding sites on this list. By default, sites added to this list will remain until removed. There are options to choose a time limit as a default for removing it after the specified time.

Once you have changed any of these settings, click the "**Save**" button.

8.1.4.2 Allowlist

Enter the URL of the website you would like to allow in the text box below and click the "**Add URL**" button. You may enter a maximum of 1000 website URLs across all profiles. Each URL may be a maximum of 255 characters in length. To remove a website URL from the Allow list, select the URL and click the "**Remove**" button located at the bottom of the page. When you are finished, click the "**Done**" button.

Enter URL (ex: domain.com) – field to enter the domain or URL to allow.

URL Timeout – select how long you would like the URL to remain on the list.

Global – Option to apply rule across all filtering groups

Keyword/Safe Search – if you would still like to have keyword and safe search enforcement applied to the domain being bypassed.

Once you have entered in a URL or domain, click the "**Add**" button.

URL Filter – This feature allows you to search through the list. You can enter part of the domain like Google to see any URLs that are in this list with that word in it. You can click Apply to view entries in this list. To clear the filter, delete the entry in this field and click Apply.

Sorting – You can click on the URL word to sort the list alphabetically.

Removing –Remove a URL by selecting the checkbox next to the URL and click the Remove button at the bottom.

8.1.4.3 Custom Allow list Categories

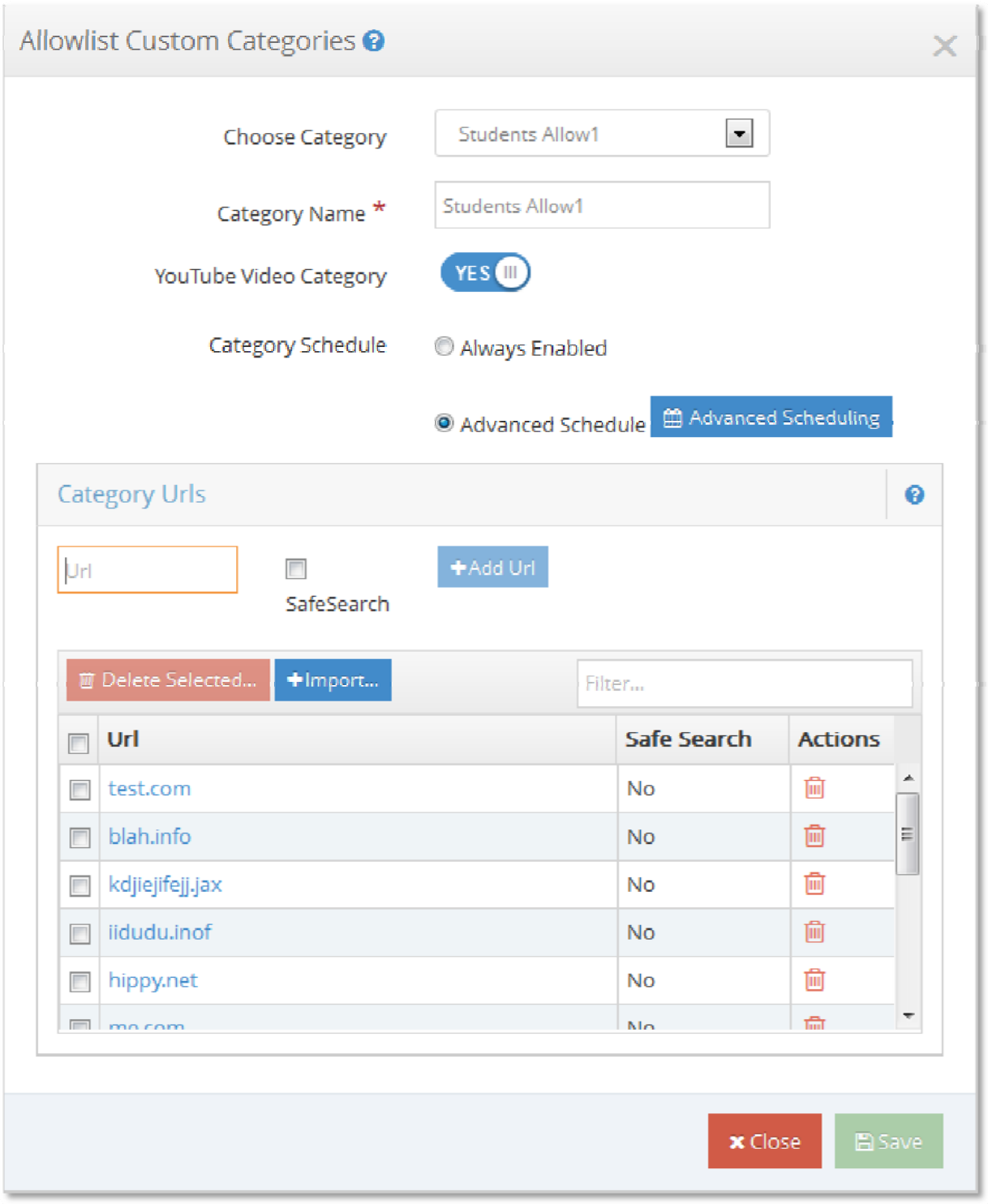


Figure 83 – Custom Allow list Categories

Select the custom allow list categories to apply to this group. These categories allow you to create custom lists of URLs that can be applied to multiple groups. Use the custom category feature to avoid adding the same URL to multiple groups.

This feature allows you to create custom Allow list categories.

Enter the URL of the website you would like to add in the currently selected category then click the "**Add URL**" button. Any group that has this category checked will have the URLs in this category applied.

YouTube Video Category – This option allows you to allow specific YouTube videos while the Audio/Video category still blocks the YouTube site.

Apply Keyword/Safe Search – Allows the domain or URL, but apply Keyword comparison and Safe Search.

8.1.4.4 Allowlist Import

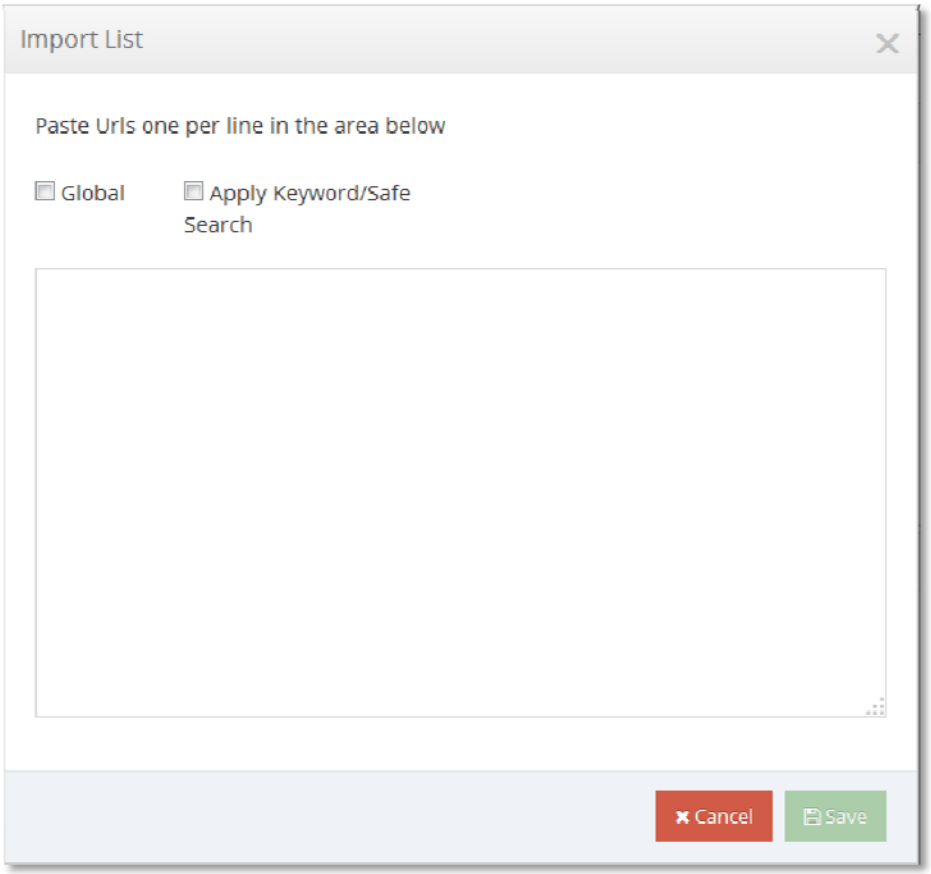


Figure 84 – Allowlist Import

You may import a list of domains to import. To import on the Allowlist or custom Allowlist, click the **Import** button. Please paste URLs one per line with a maximum of 255 characters per domain/IP/URL. Once you are done, click the "**Save**" button.

8.1.5 Block Specific Websites

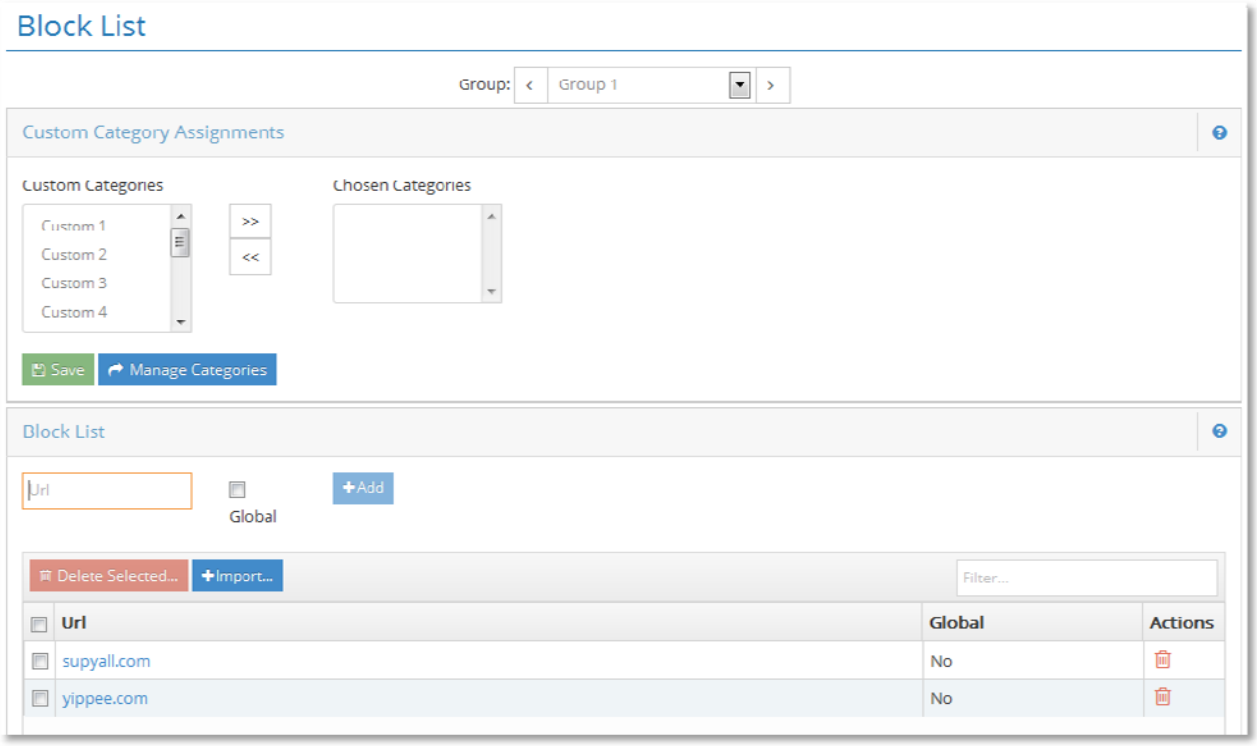


Figure 85 – Block Specific Websites

This page allows you to block specific website URLs from being accessed on your network.

Enter the URL of the website you would like to block in the text box below and click the "**Add URL**" button. You may enter a maximum of 1000 website URLs across all profiles. Each URL may be a maximum of 255 characters in length. To remove a website URL from the Block list, select the URL to remove and click the "Remove" button located at the bottom of the page. Click the "Done" button when you are finished.

8.1.5.1 Custom Block list Categories

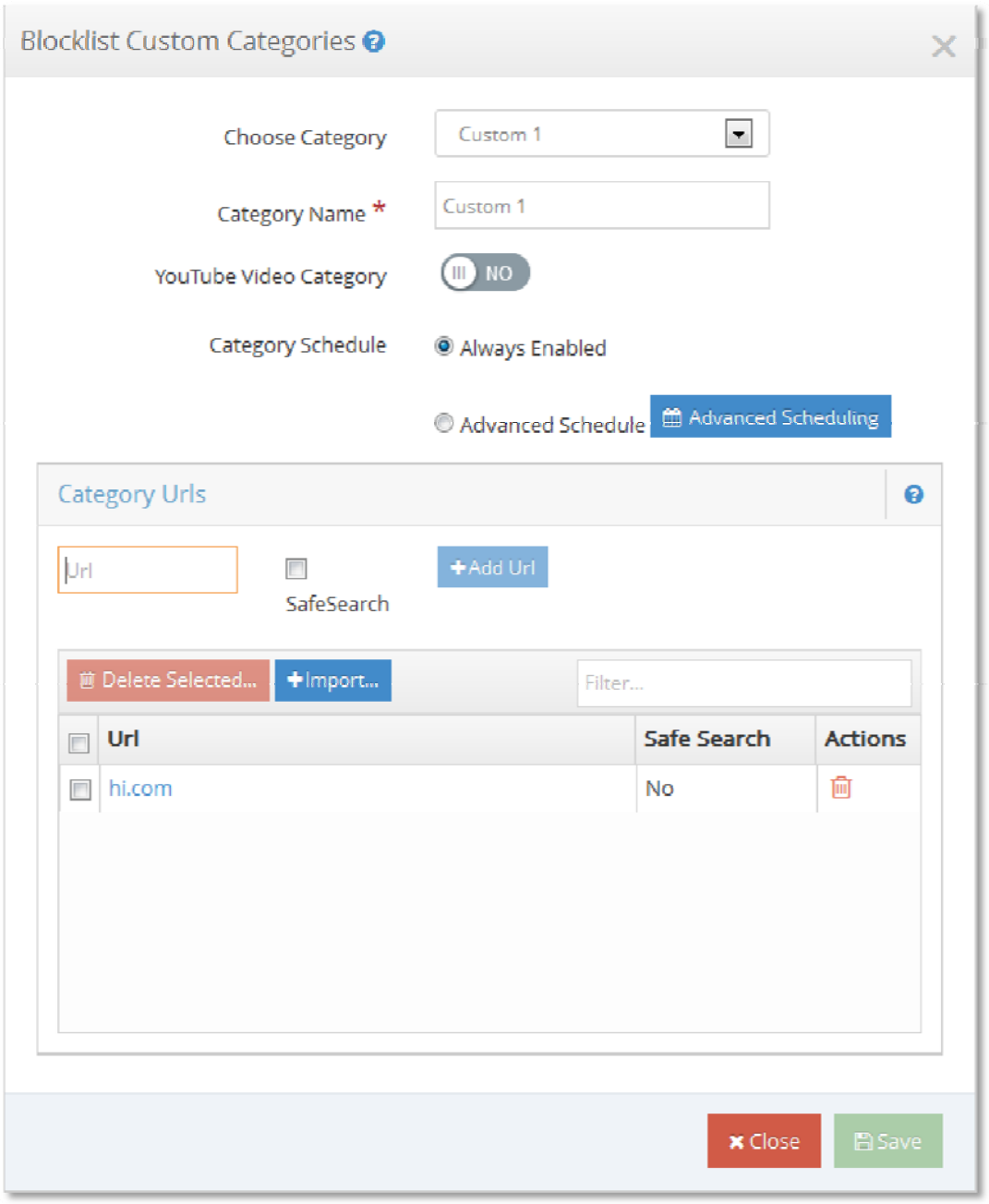


Figure 86 – Custom Block list Categories

Select the custom block list categories to apply to this group. These categories allow you to create custom lists of URLs that can be applied to multiple groups. Use the custom category feature to avoid adding the same URL to multiple groups.

This feature allows you to create custom Block list categories.

Enter the URL of the website you would like to add the currently selected category in the text box below and click the "Add URL" button. Any group that has this category checked will have the URLs in this category applied.

8.1.5.2 Block list Import

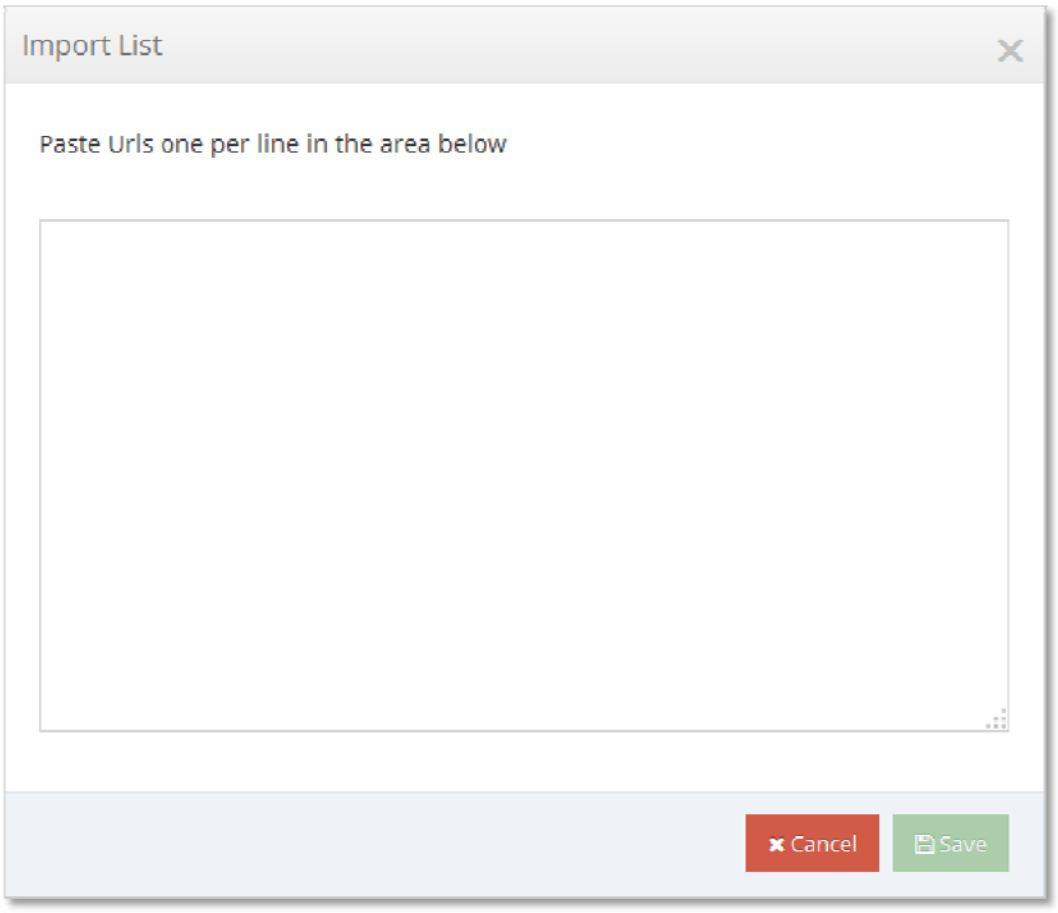


Figure 87 – Block list Import

You may import a list of domains to import. To import, click the +**Import** button. Please paste URLs one per line with a maximum of 255 characters per domain/IP/URL. Once you are done, click the “Import Now” button.

8.1.6 Keyword Blocklist / Allowlist

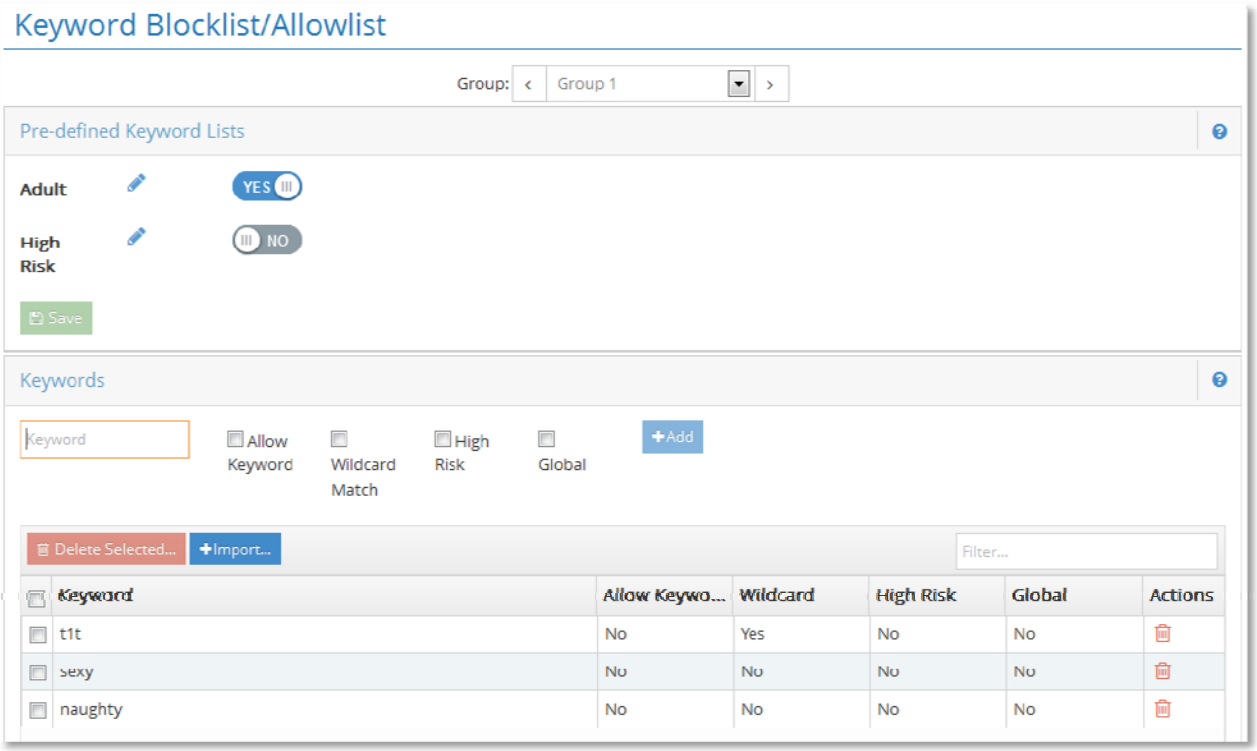


Figure 88 – Keyword Blocklist / Allowlist

This feature allows you to create keyword Block lists. The iboss will block Internet sites that contain these specific keywords in the URL. In addition, web searches using the keywords in the list(s) will also be blocked.

8.1.6.1 Pre–Defined Keyword Lists

You may select from pre–defined keyword category lists. Each category contains its own keyword list. To enable a keyword list, select the checkbox next to the category. You may view and edit the list by clicking on the pencil icon to edit the list. When you are finished, click the "**Save**" button.

High Risk – The words on this list will send the administrator of the group an email notification when searched.

8.1.6.2 Keywords

Enter the custom keyword that you would like to block in the text box below and click the "**Add**" button. You may enter a maximum of 2000 URL keywords across all profiles. Each keyword may be a maximum of 19 characters in length (letters and digits only). To remove a keyword from the list, select the keyword and click the "**Delete Selected**" button located at the bottom of the page.

Allow Keyword – Checking this option will allow the word if it is in the URL within a keyword parameter.

Wildcard Match – Checking this option will use wild card matching on the keyword. When wild card matching is used, the entire URL is searched for the keyword pattern. If wild card matching is not used, the iboss will analyze the URL for queries containing the keyword(s) entered.

High Risk – This option will send a notification to the group administrator when searched for.

Global – This option will span across all filtering groups when selected. When removing a “Global" entry, it will remove the entry from all filtering groups.

Keyword Searching – You can use the search filter input box to the right to filter the keyword list view.

You can import a list of keywords to block by clicking “**Import**”. You may remove keywords by checking the keyword and clicking the “**Delete Selected**” button.

8.1.6.3 Keyword Import

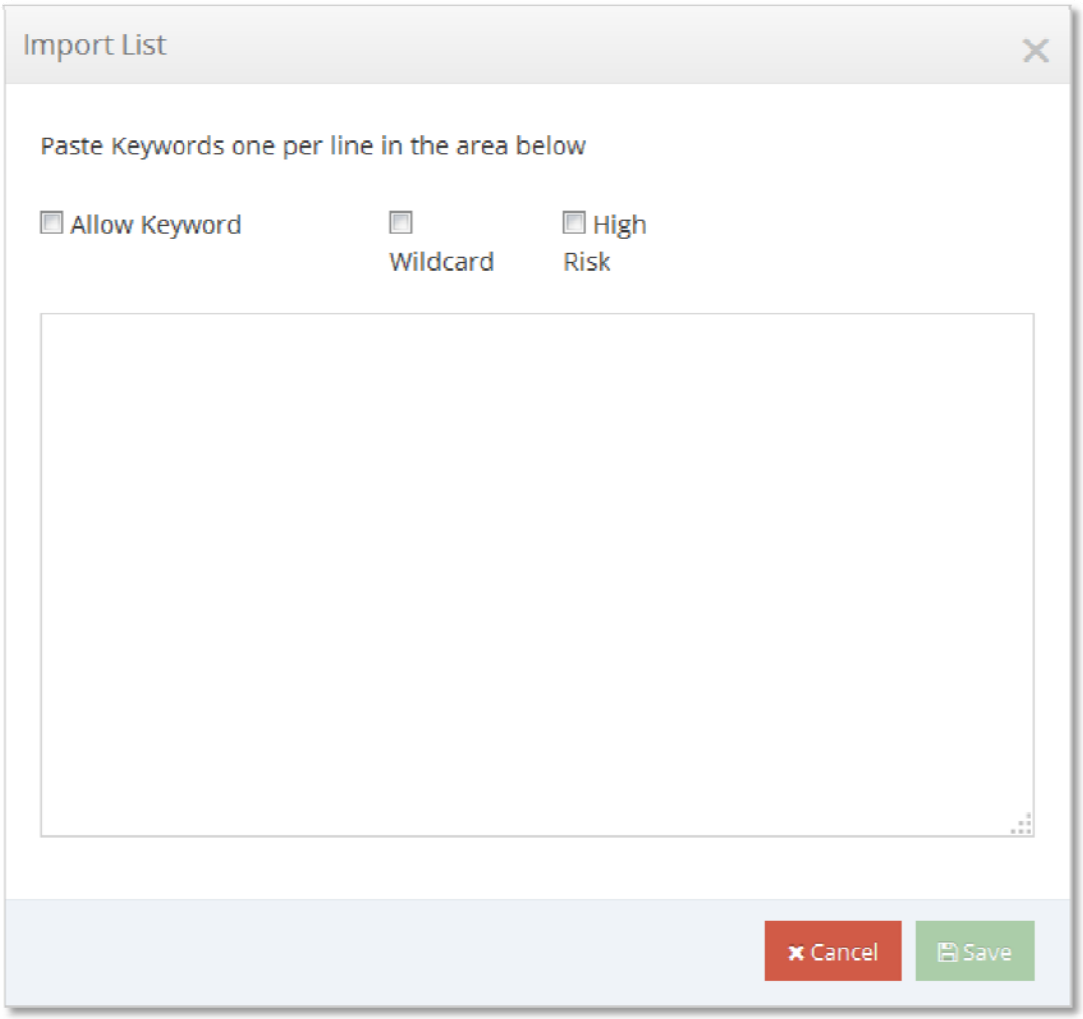


Figure 89 – Keyword Import

You may import a list of keywords to import. Please paste keywords one per line with a maximum of 19 characters per keyword. You may select Allow Keyword, Wildcard, and High Risk when importing. Once you are done, click the **Save** button.

8.1.7 Bandwidth Shaping

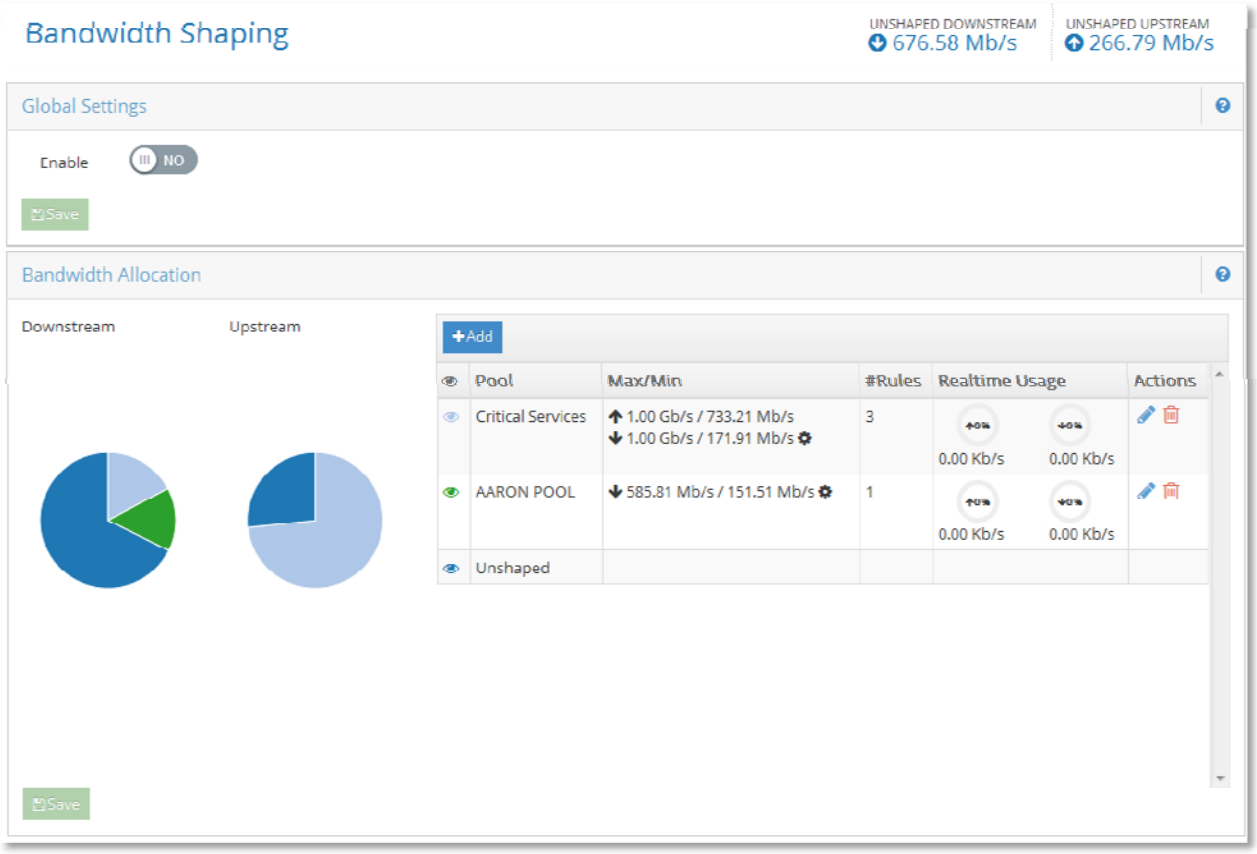


Figure 90 – Bandwidth Throttling

There is a separate, more comprehensive manual for the Bandwidth Throttling/QoS feature.
Please request this from iboss Support for the iboss Enhanced QoS & Bandwidth Shaping Datasheet.

8.1.8 Port Blocking

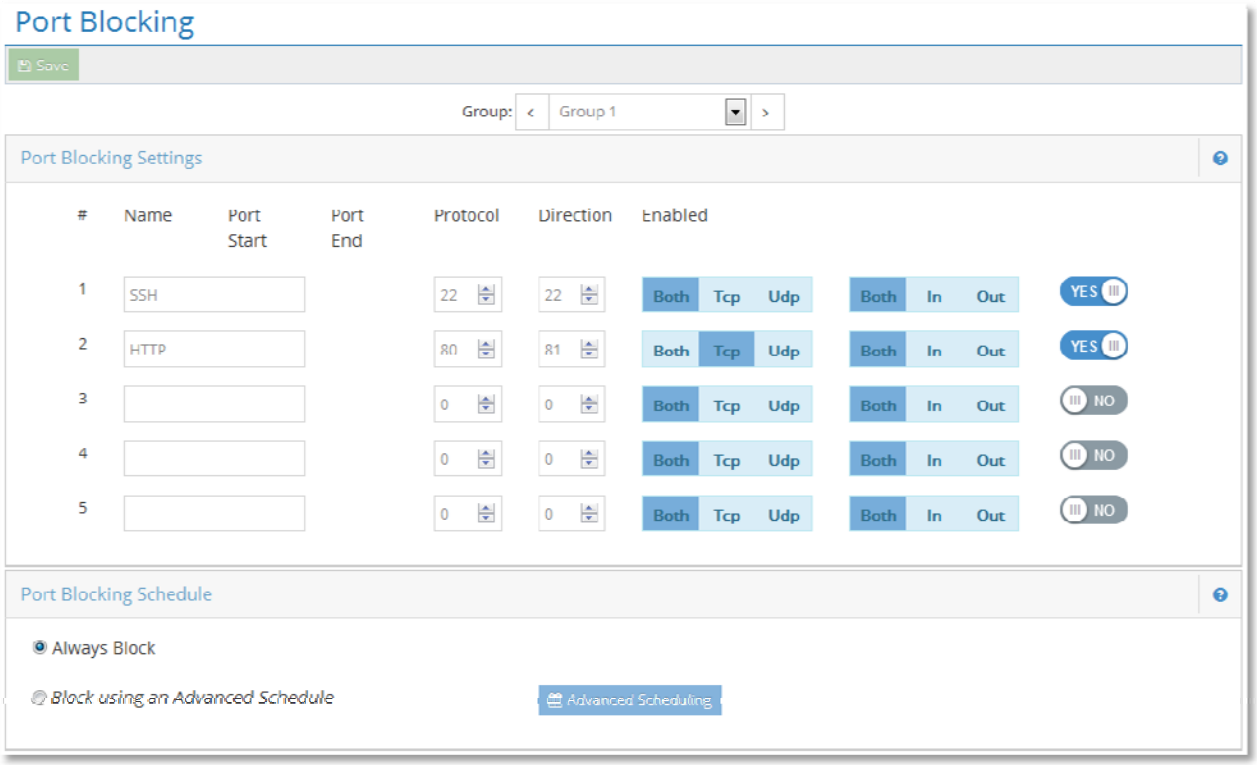


Figure 91 – Port Blocking

Port blocking allows Internet traffic on specified ports, or ranges of ports to be blocked from accessing the Internet. Traffic using the specified ports will be blocked completely. This allows you to enter the name, port start, port end, protocol, and direction. Once you enter in the information click Enable and save.

Port Blocking Schedule – You may choose to block these ports all the time or Block on an Advanced Schedule.

8.1.9 Content/MIME Type Restrictions

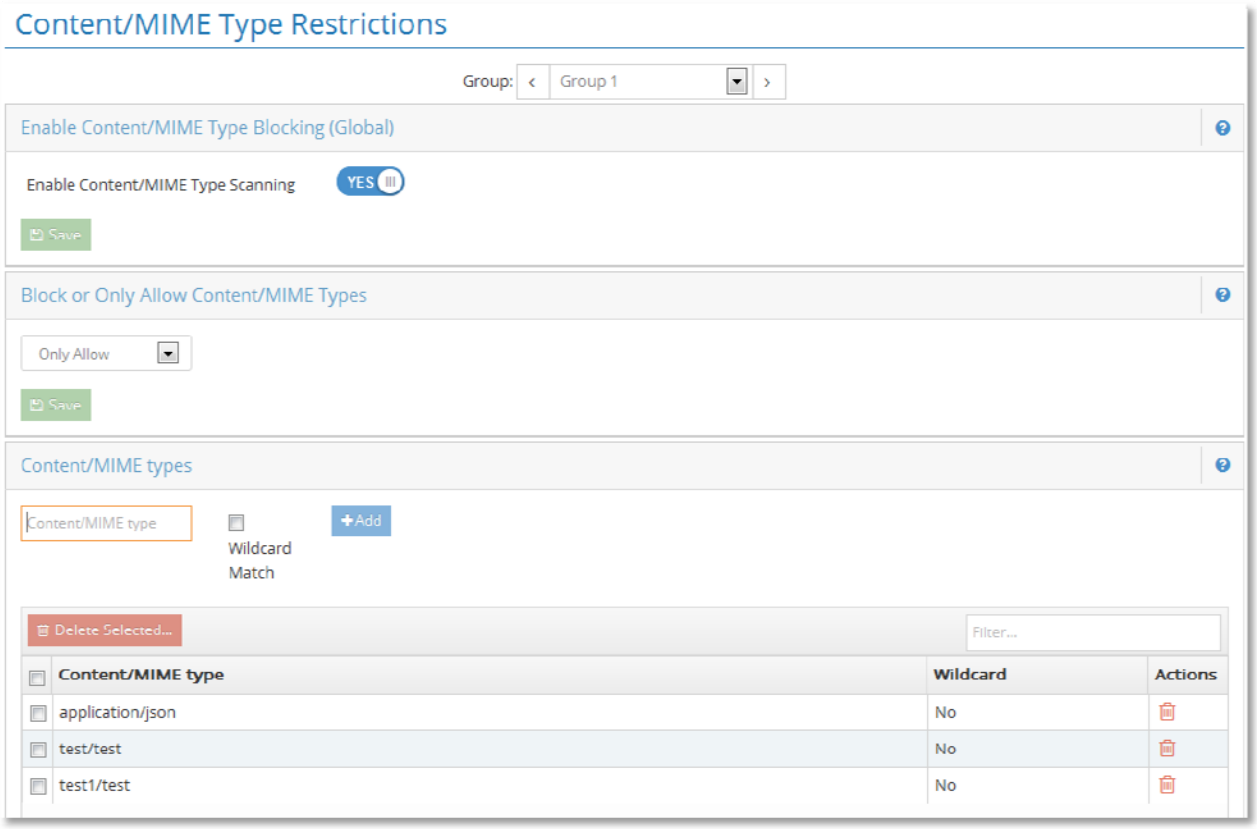


Figure 92 – Block Content/MIME Types

This page allows you to block web content based on Content Type or MIME type. You can enter a content type like audio/mp3 to block this type of content. There are MIME type lists online that can be used for reference. You can enter wildcard matches for different file types instead of using the file extensions. For example, you can type in **audio** and check the box for Wildcard Match to block all audio type files.

You also have the choice to **Block** the entries in the list, or **Only Allow** the entries in the list.

After you enter a content/MIME type, click **Add** to add it to the list. To remove it, select it with the checkbox next to the entry and click the **Remove** button at the bottom.

8.1.10 File Extension Blocking

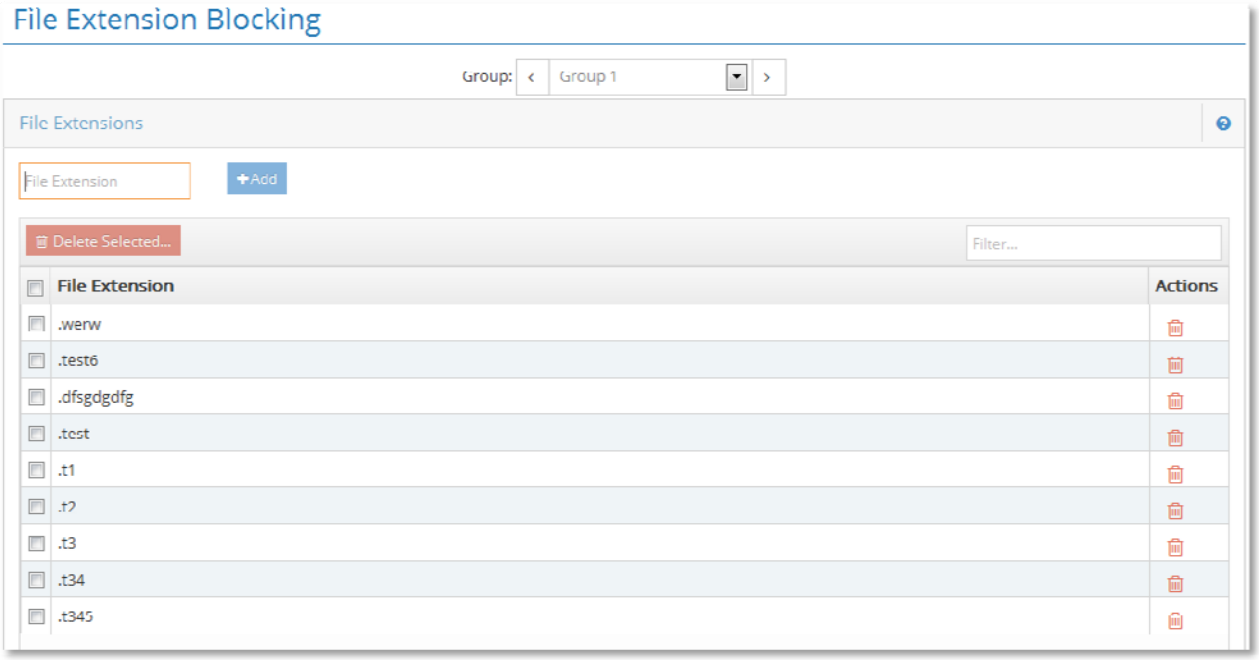


Figure 93 – File Extension Blocking

This page allows you to block specific file extensions from being downloaded on your network.

Enter the file extension of files you would like to block in the text box below and click the "**Add**" button. You may enter a maximum of **2000** file extensions across all profiles. Each extension may be a maximum of **15** characters in length. To remove an extension from the Block list, select the extension to remove and click the "**Remove**" button located at the bottom of the page. Click the "**Done**" button when you are finished.

8.1.11 Domain Extension Restrictions

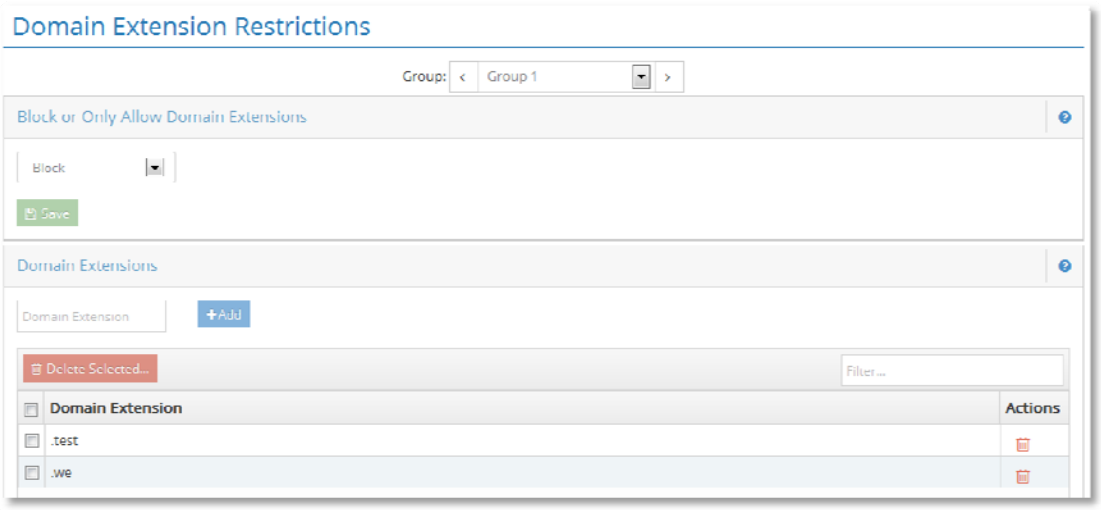


Figure 94 – Domain Extensions Restrictions

This page allows you to block or allow specific domain extensions from being accessed by a particular group. You may choose to **Block** the domain extensions in the list or to **Only Allow** the extensions in the list. If you choose to only allow the domain extensions in the list, then any domain whose extension is not in the list will be blocked. Alternatively, if you choose the block the extensions in the list, then all access to all other domain extensions will be allowed. For example, you may choose to allow only domains that end in ".com" and ".net". Any domain that does not end with those extensions will be blocked.

Enter the domain extensions in the text box below and click the "**Add**" button. You may enter a maximum of **2000** domain extensions across all profiles. Each extension may be a maximum of **15** characters in length. To remove an extension from the list, select the extension to remove and click the "Remove" button located at the bottom of the page. Click the "Done" button when you are finished.

Note: These settings do not apply to web access to direct IP addresses. You can block direct IP address access by going to Internet Controls> Block Specific Web Categories> IP Address blocking.

8.1.12 Sleep Schedule

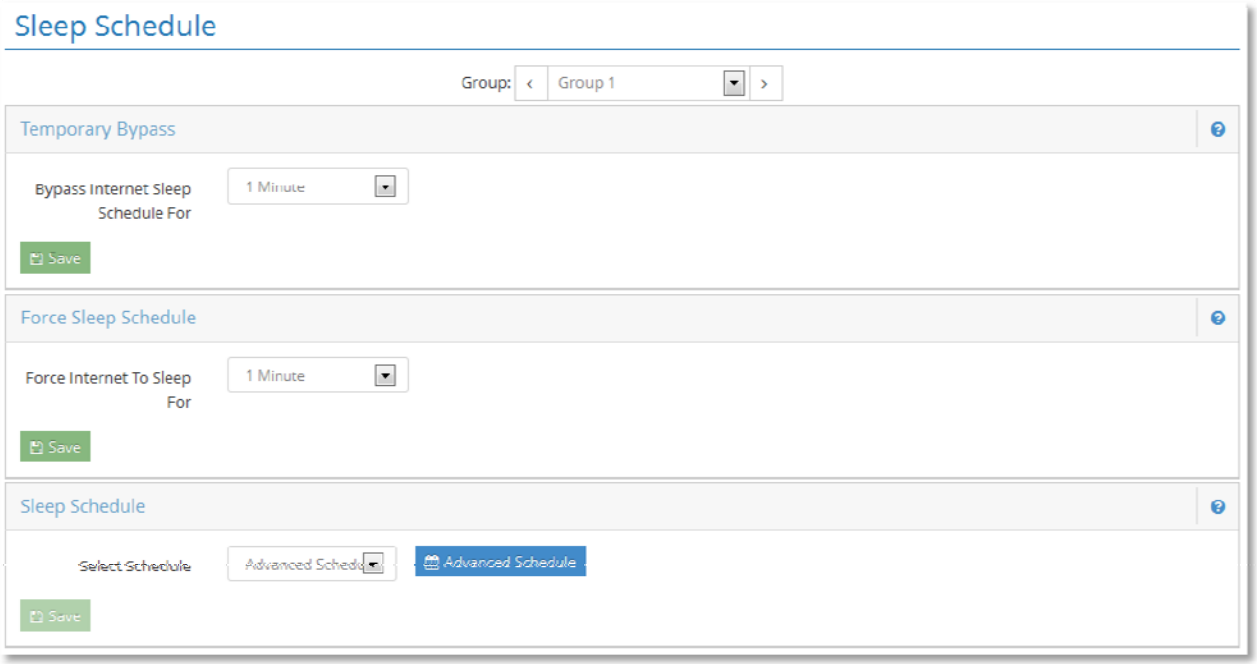


Figure 95 – Sleep Schedule

Internet Sleep Mode allows you to put your Internet connection to sleep (disabling all Internet traffic to and from a particular group). This is beneficial for when the Internet doesn't need to be on or accessed.

You may manually force the Internet to sleep by selecting a time period under the "**Force Internet To Sleep For:**" section and pressing the "**Sleep Now**" button. You may also bypass the sleep schedule by selecting a time period under the "**Bypass Internet Sleep Schedule For:**" section and pressing the "**Bypass Now**" button.

When manually forcing the Internet to sleep or bypassing the sleep schedule, a countdown timer will show that will allow you to cancel the forced sleep or cancel the bypass.

You may setup a daily schedule or an Advanced Schedule by which to put the Internet to sleep under the “**Sleep Schedule**” section.

When the Internet is in Sleep Mode, the "**Internet Sleep Mode**" page will be displayed in the web browser if Internet access is attempted. To customize the message that appears on the "**Internet Sleep Mode**" page, go the custom block page messages under preferences. You may override Internet Sleep Mode and wake up your Internet connection by entering the iboss login password into the "**Internet Sleep Mode**" page when it is displayed.

8.1.12.1 Sleep Mode Page

When a page is blocked from violation of the iboss sleep mode schedule, this page will show up in the web browser to the user. You may manually login and turn off Internet Sleep Mode by typing in the password and pressing Login. The Sleep Mode will continue at the next scheduled time..

8.1.13 Real–Time Monitoring / Recording

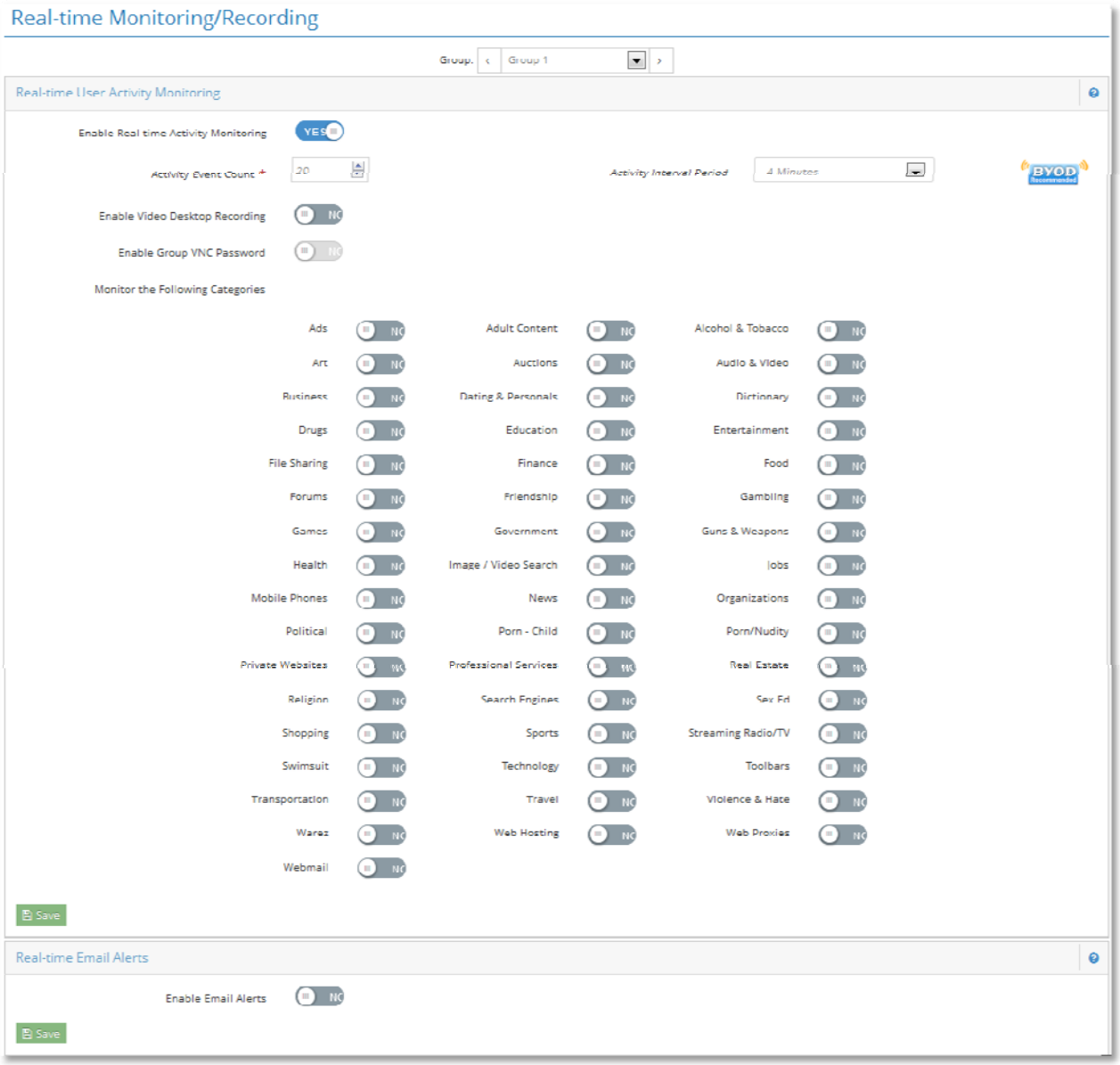


Figure 96 – Real–time Monitoring / Recording

Note: The VNC recording feature is not included by default and may not be available on all models. It is a feature add–on upgrade.

This feature allows you to adjust the settings for real–time user activity monitoring feature. The iboss can monitor user activity in real–time and send email alerts, or perform desktop video recordings when a predefined level of activity is reached. This allows you to have 24/7 awareness of network activity.

User activity monitoring must be enabled for the group in order for the settings to take effect. If real–time user activity monitoring is disabled, monitoring by trigger thresholds is disabled for all computers in the group.

Real–time User Activity Monitoring – This setting enables trigger based real–time monitoring for the group. If this setting is disabled for the group, any additional options for this page have no effect.

Trigger Level And Interval – Trigger when specified number of events occur within a chosen time period.

Real–time Email Alerts – This setting will cause the iboss to send an email alert when the above threshold criteria is reached. The alert will occur when the trigger is reached to allow you to respond when certain activity is occurring.

Note: The email address that these alerts are going to be sent to can be configured below for this group or in the Settings section of the Reports interface.

Group Email Contact – This is the email where real–time alerts will be sent for activity related to the currently selected group. If left blank, the email address specified in the reporter under settings will be used for alerts related to this group. Use a semicolon between email addresses to specify more than one email address.

Send Alert When User Enters Group – This setting will cause the iboss to send an email alert whenever a user enters into this filtering group. Alerts will only be sent when a user logs in manually with override and will not be sent when a user is authenticated transparently.

Send Alert When User Leaves Group – This setting will cause the iboss to send an email alert whenever a user exits from this filtering group.

Video Desktop Recording – This setting enables a desktop recording to occur when the above threshold criteria is reached. In addition, you can specify the duration of the desktop recording.

The computer must be registered with the iboss and have VNC enabled for this setting to take effect. In addition, the computer must have a compatible VNC application installed and running. This is where you will specify how long to record the video.

Include The Following Categories – This is where you choose the categories to include in the trigger thresholds.

8.1.14 Exception Requests

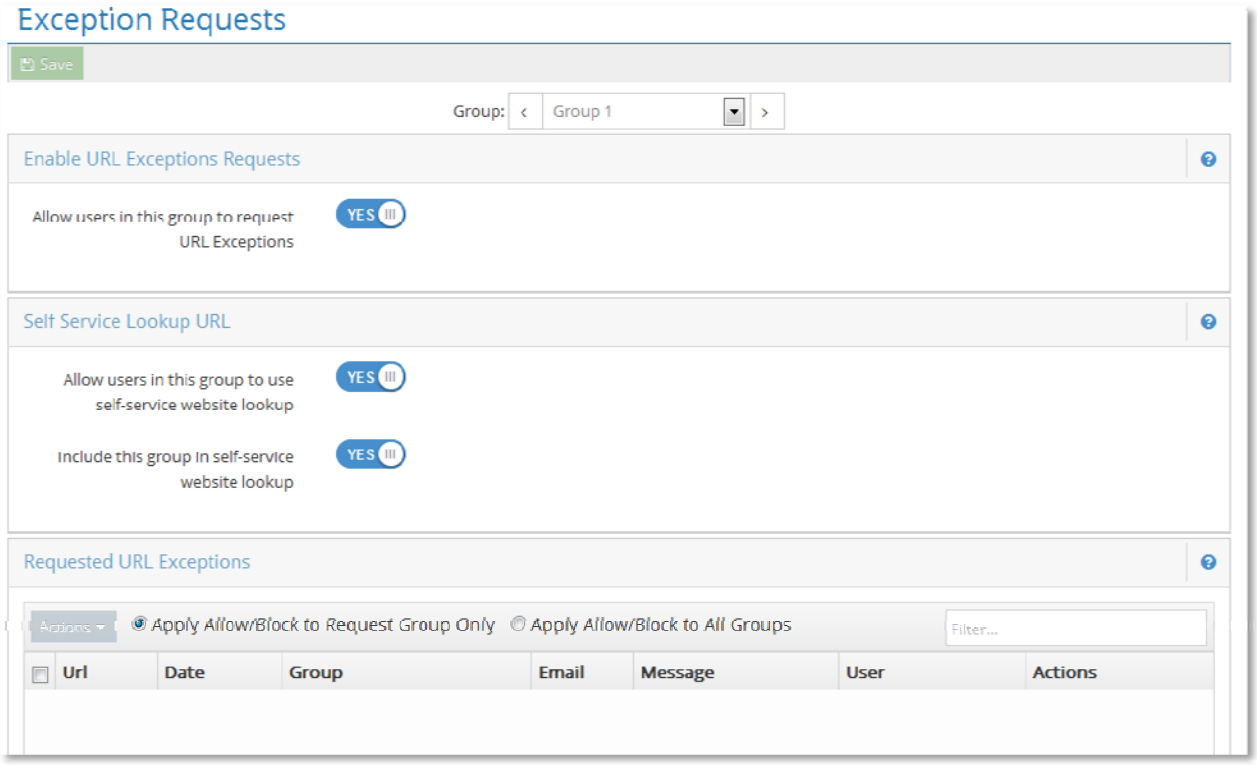


Figure 97 – Exception Requests

If enabled this feature adds a section to the block page allowing the user to submit a request to allow the page. Notes and the user's email may be included. The request will be delivered to the email address(es) specified at Controls → Monitoring in the section 'Group Email Contact' if one is specified for the group; otherwise it will be delivered to the email specified in the settings of the reporter.

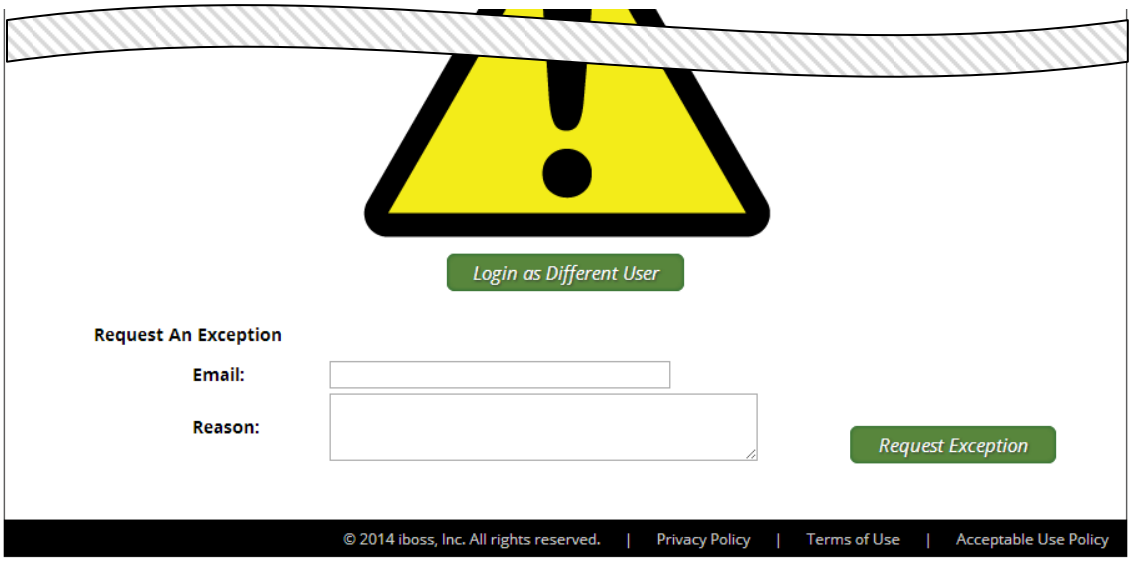


Figure 98 – URL Exception Request – Block Page

8.1.15 URL Lookup

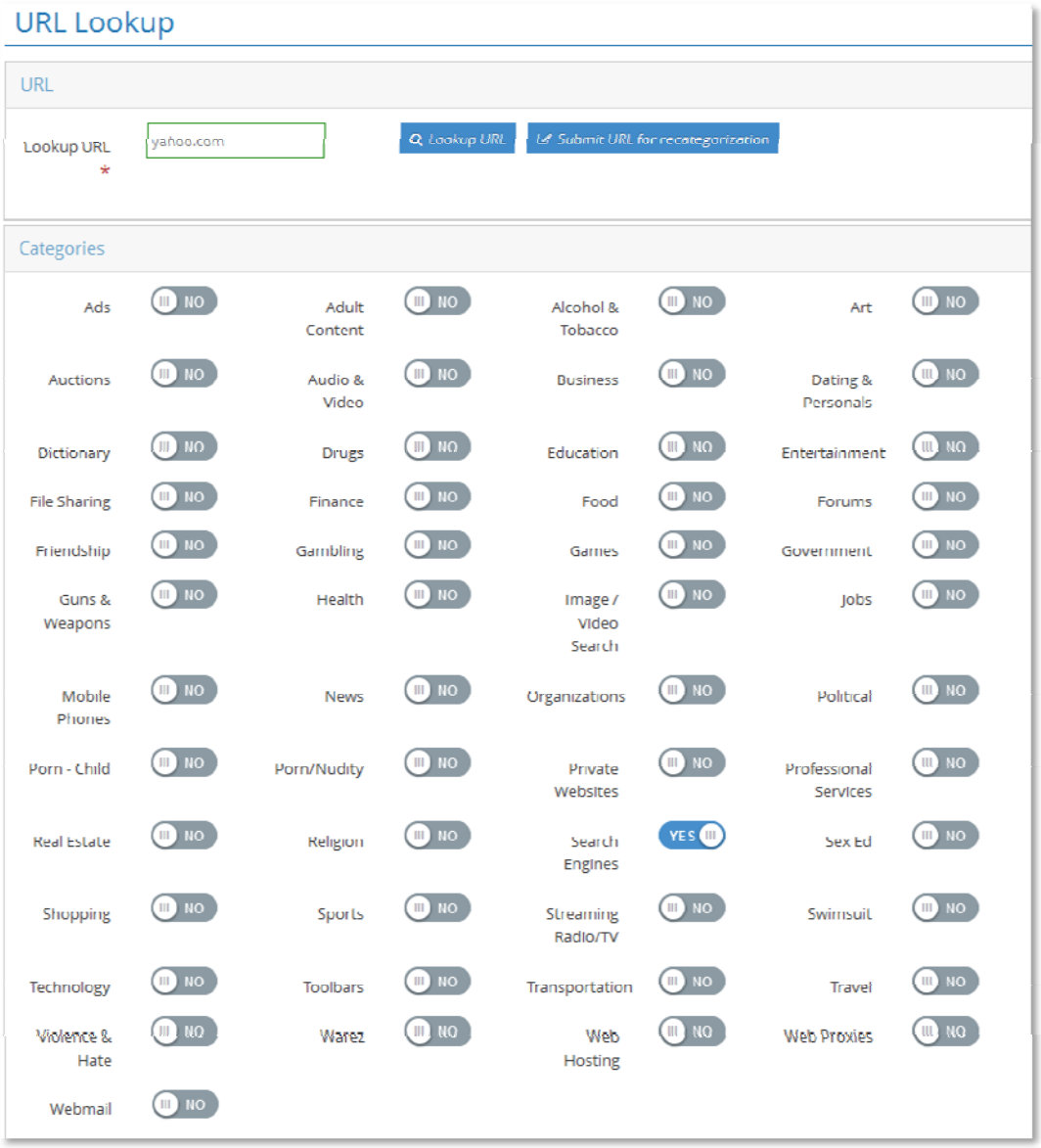


Figure 99 – URL Lookup

This page provides a utility to query a URL to see how it has been categorized. Once a URL has been entered and the 'Lookup' button clicked, there will be a message at the top of the screen indicating the database status of the URL. The section below will indicate which categories it is assigned.

10.1 Filtering Groups

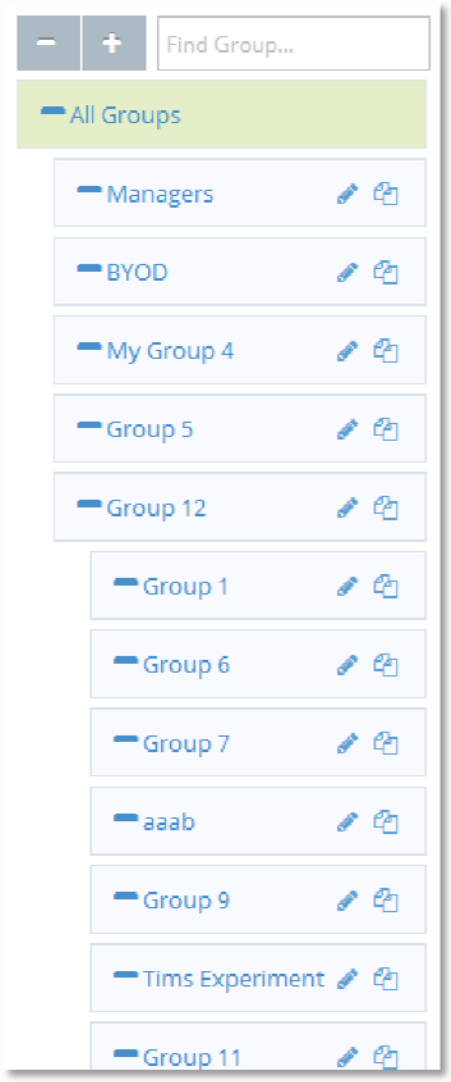


Figure 115 – Filtering Groups

This section shows the Filtering groups that are setup in the SWG filter. The Filtering groups can be created in a hierarchal format to easily group different filtering groups together. A user or computer would still only fall under one filtering group and does not inherit filtering policies from parent groups. The allowed number of filtering groups has been created for you.

Filtering groups are used to apply Internet filtering rules to computers and/or users on your network. You may customize the group names to easily identify its purpose. Group names may be up to 50 characters in length.

You can move filtering groups in the tree for easier viewing by clicking and dragging the filtering group.

10.1.1 Edit Filtering Group

Figure 116 – Edit Group

To edit the filtering group, click the pencil icon next to the filtering group name.

Group Name – You can configure the Group Name to match Security Group names or OU group names. This is determined based on your directory integration options for sending group names.

Alias Group Names – You can enter multiple group names in this field (one per line) that will match directory group names. These groups that match will be grouped together to fall under the same filtering group policy.

Logging – This option enables logging for this filtering group.

Priority – If a user matches multiple filtering groups within the iboss, the one with the highest priority number will take precedence. .

Override Group – An iboss filter group may be designated as an 'Override Group' which can be used as a method of temporarily changing to a different filtering group. This filter group should be given a priority higher than any non–Override filter groups a user may belong to. The Override Group will never be assigned via transparent login. A user presented with a block page may revalidate his/her credentials and be "bumped" up to the override group until logging out or 'Override Timeout' is reached.

Override Timeout – This timeout field will move the user back to their original filtering group when this time is reached.

NOTE	This field allows you to add notes to the filtering group.

Once done configuring the settings, click the "**Update Group**" button.

10.1.2 Copy Group Settings

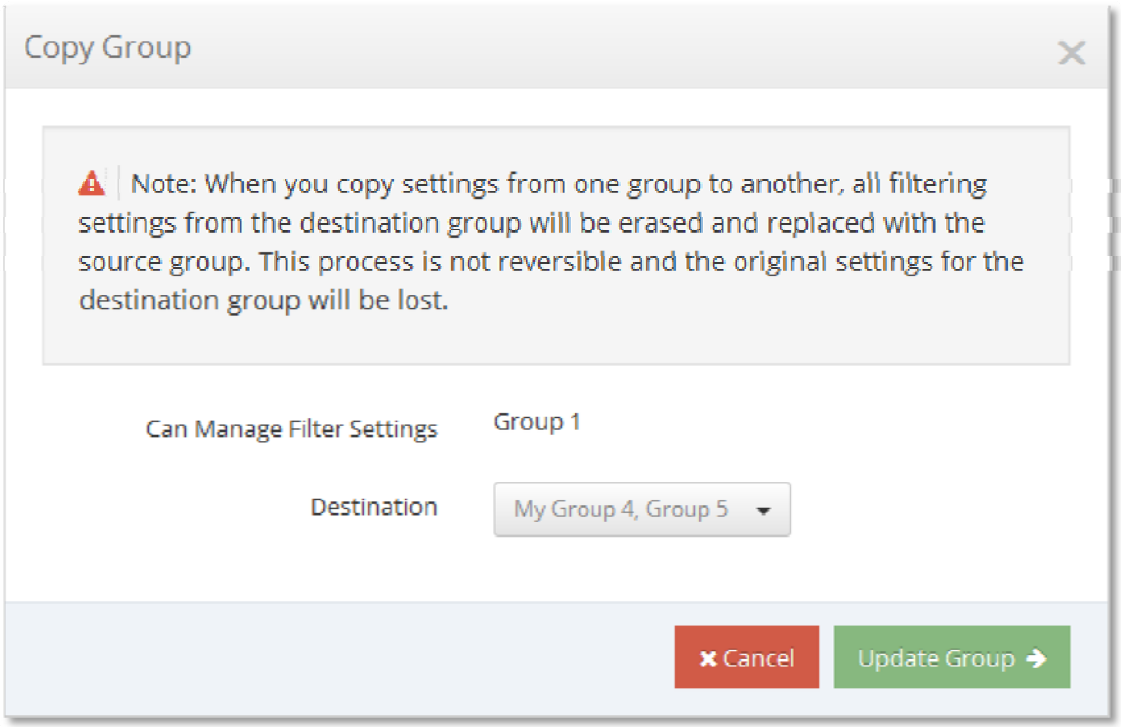


Figure 117 – Groups – Copy Group Settings

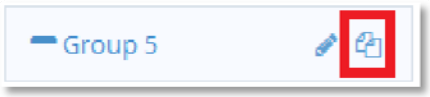


Figure 118 – Copy Group Icon

To copy group settings from one group to another, click the double document icon to pull up the Copy Group Settings.

The Copy Group window allows you to quickly copy filtering settings from one group to another, or several. Select the group to copy settings from and a group to copy settings to and then click the Update Group button. This will completely overwrite the destination and provides a configuration starting point but there is no connection between the groups from this point.

NOTE	This process is not reversible and the original settings for the destination group will be lost.

10.1.3 Group – Computers & Users Tabs

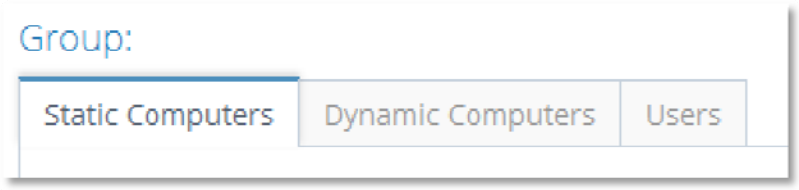


Figure 119 – Group – Computers & Users Tabs

The Groups section has tabs at the top to switch from Static Computers, Dynamic Computers, and Users for each select group or All Groups.

Static Computers – The computers listed under the Static Computers are Manually Identified Computers and fall under the filtering group that is selected..

Dynamic Computers – The computers listed under the Dynamic Computers are computers that have been detected going through the iboss and fall in the filtering group that is selected.

Users – The users listed under the Users tab are Users that have been manually added to the SWG and assigned to the filtering group that is selected.

10.1.1 Add User

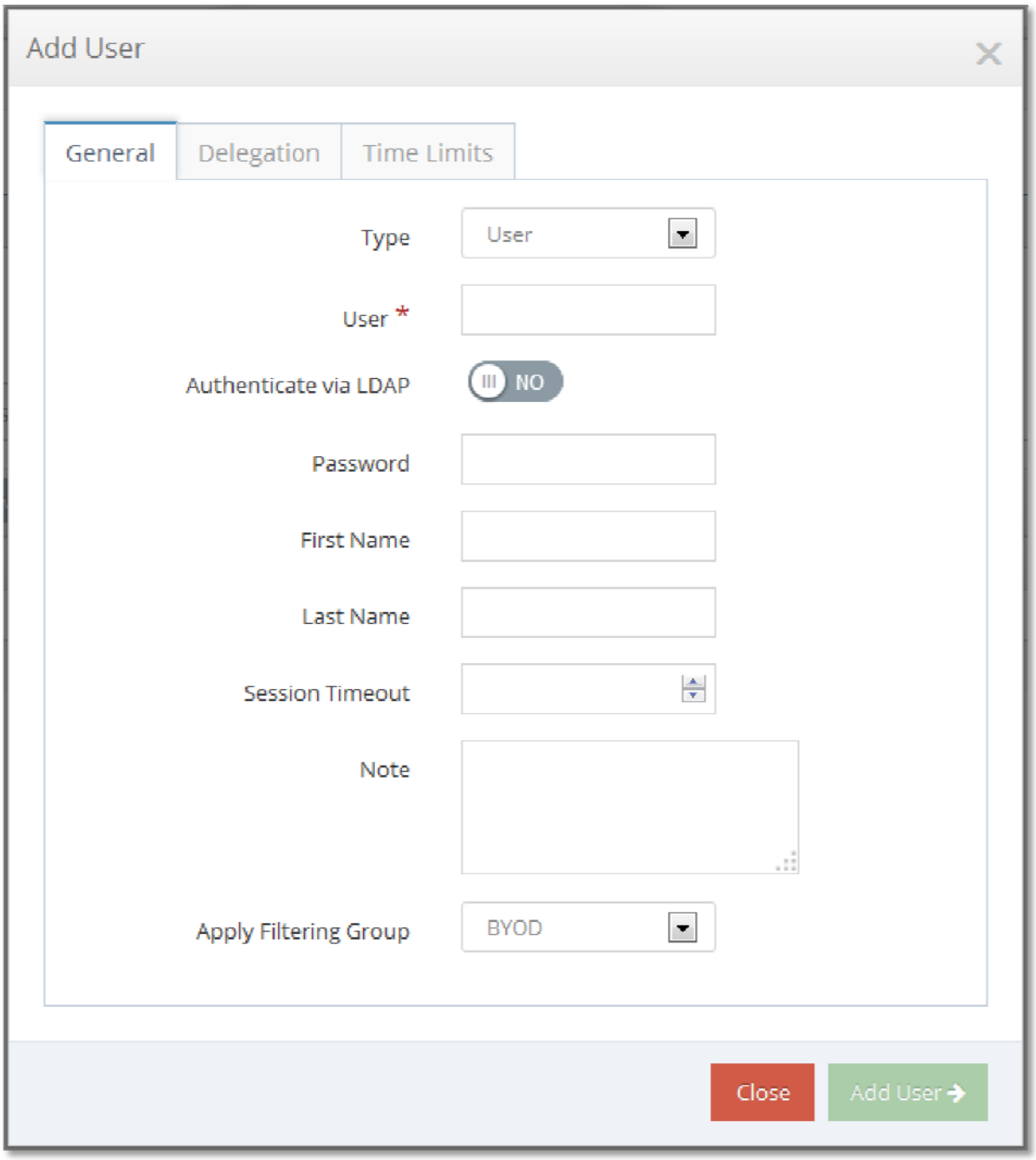


Figure 120 – Add User

To add a new user, click the Add User button at the top.

These users will not have access to the iboss settings and cannot log onto the iboss to change settings unless "**Delegation Settings**" are enabled.

10.1.1.1 General

Type – You can select User or Admin Login AD/LDAP Group. Selecting Admin Login AD/LDAP group allows administrator logins to the iboss from an AD or LDAP group.

User – Enter the username or group name in this User field.

Authenticate via LDAP – You can enable this option to authenticate the user via LDAP to use the user's password within LDAP.

Password – Set the password for the user if you do not have Authenticate via LDAP option selected.

First Name – Enter the user's first name.

Last Name – Enter the user's last name.

Session Timeout – Enter the amount of minutes until the user is logged out of the Internet Access Window. The default is 0 which will not log the user out automatically with this option.

Note – This allows you to enter a note for the user.

Apply Filtering Group – This option allows you to specify which group the user will fall under when they authenticate. You can also select No Filtering which is the last option to bypass filtering for this user.

10.1.1.2 Delegation

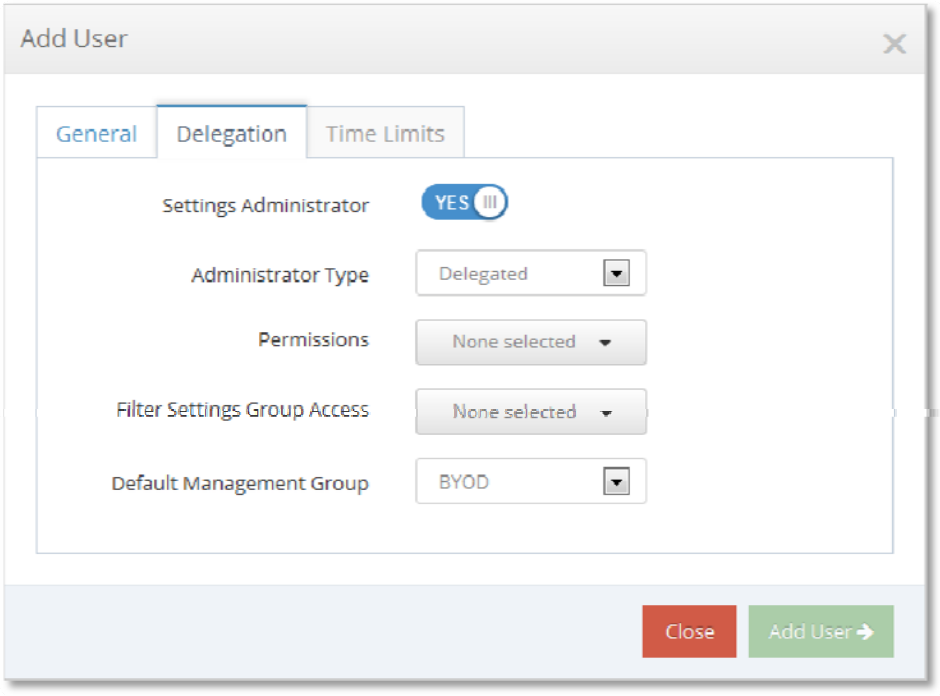


Figure 121 – Users – Delegation

When adding a user to the iboss, you will also have options to give them access to filtering settings.

Settings Administrator – Option to enable delegated administration.

Administrator Type – Full allows full access to the iboss SWG Filter. Delegated allows you to specify which permission settings and which groups the user can manage.

Permissions – Select which filter control settings the user is allowed to manage. You can select multiple settings.

Filtering Settings Group Access – Select which filtering groups the user is allowed to manage.

Default Management Group – This is the default management group that the user is administering.

10.1.1.3 Time Limits

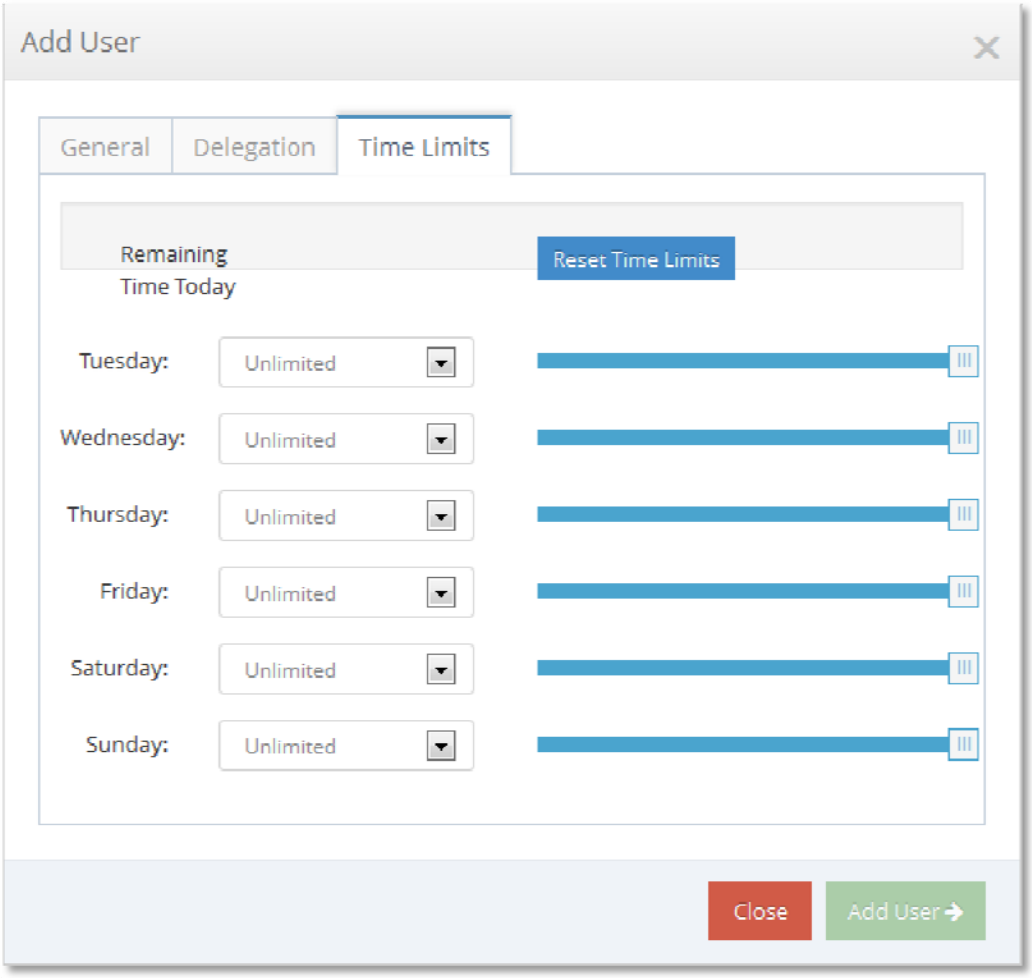


Figure 122 – Users – Time Limits

This will allow you to set daily time limits for each day of the week for a user. You can set a time between 15 minutes to 23 hours that a user can be logged in from throughout the day. This means that when a user has the allocated time throughout the day to use the time limit. When finished click the "**Add User**" button. If you want to cancel your changes click the "**Close**" button.

10.1.2 Add Computer

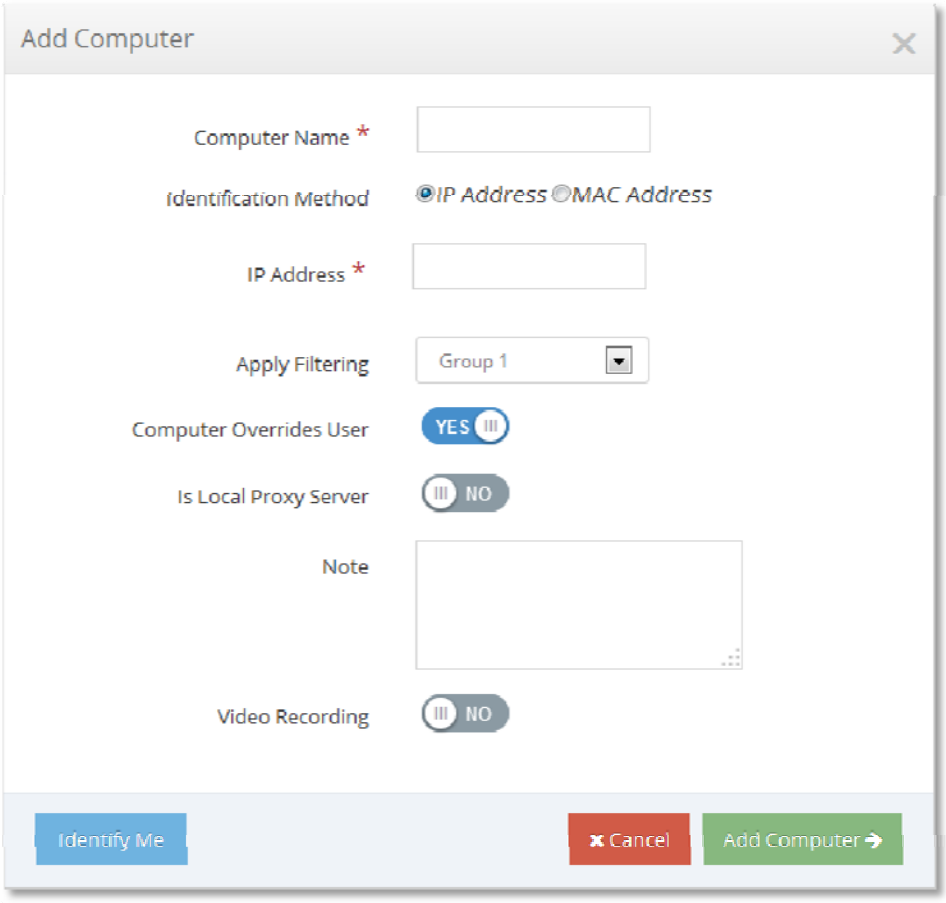


Figure 123 – Add Computer

To identify the computer you are using now, click the "**Add this computer**" button. Advanced users may click the "**Add Computer**" button to manually identify a computer. For the "**Add Computer**", you will need to know the IP address or MAC address of the computer you wish to identify.

Computer Name – Enter a Computer Nickname for your reference.

IP Address / MAC Address Type – If you have your local subnets setup to identify your subnet as IP address, choose IP address. MAC Addresses may not be visible to the iboss on a layer 3 routed network with internal gateways and multiple subnets.

IP Address – Enter the IP address

Apply Filtering – You may either set the Apply Filtering to "**Yes, Use Default Rules**" with one of the filtering groups, "**No, Bypass Filtering Rules**" or "**Require user login for this computer**" for the computer you are identifying.

*The "Yes, Use Default Rules" will show the assigned name of the filtering group.

Computer Overrides User – This option allows you to enforce the specified filtering policy on that computer, regardless of the rights of the person logged in.

Is Local Proxy Server – This option is to identify if the computer you are identifying as a proxy server on your local network.

Video Recording – *There are more options if you have the DMCR feature added. This will allow you to put the Port, Password and IP address of the client VNC computer. Please refer to the Controls → Monitoring section for more information.

When finished click the "Add Computer" button. If you want to cancel your changes click the "Cancel" button.

11 Tools

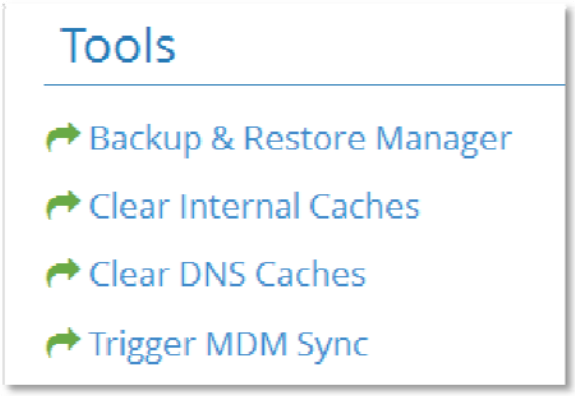


Figure 124 – Tools

This section has quick links for the Backup & Restore Manager, Clear Internal Caches, Clear DNS Caches, and Trigger MDM Sync.

11.1 Backup & Restore Manager

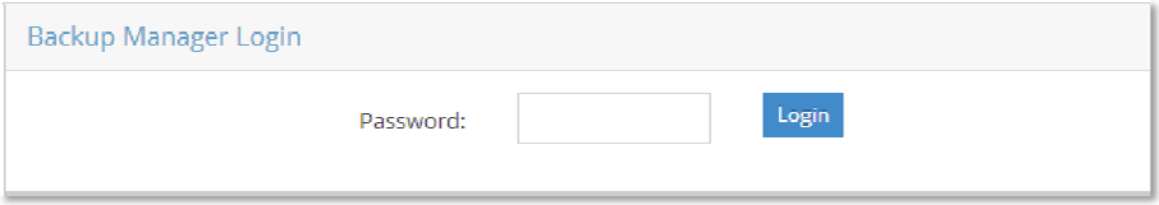


Figure 125 – Backup & Restore Manager Login

The login for this interface requires the full admin password to login.

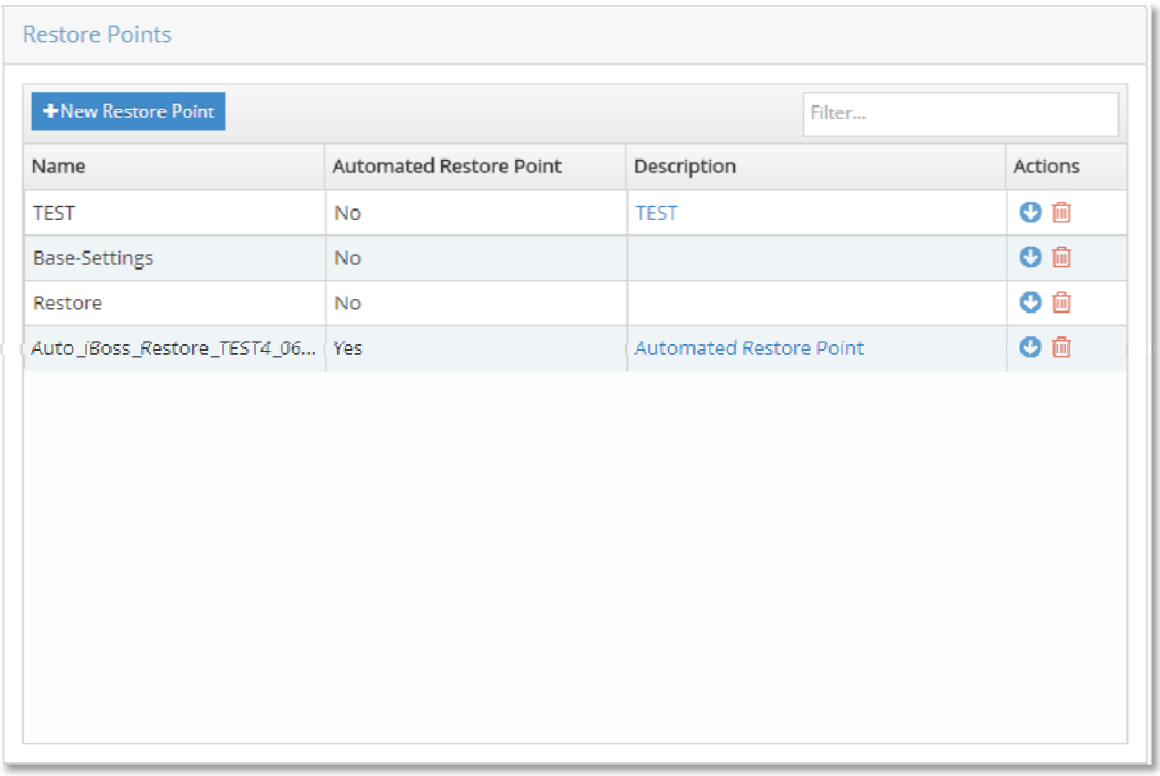


Figure 126 – Backup & Restore – Restore Points & Creating Restore Point

Once you login, you can see all the restore points that have been created. There are no restore points created by default. It is recommended to create a restore point after you have configured your controls settings and then click the Download button to copy the restore point off of the device.

When a restore point is created, you have the option to delete it off the device, download the restore point which contains all of the settings and firmware, and the option to restore the iboss device back to a specific Restore Point.

Restoring the iboss from a restore point must be from the same model of the iboss. It does revert back to the firmware version number that the iboss was on when the restore point was created.

If you have multiple iboss devices and would like to copy settings from one device to another, one thing to note is that the subscription key also gets copied and restored. This may overwrite your current subscription key for the second unit. If this is the case, you will want to save the restore point of the second iboss device and after restoring an imported restore point, overwrite the subscription key with the original subscription key that was there prior.

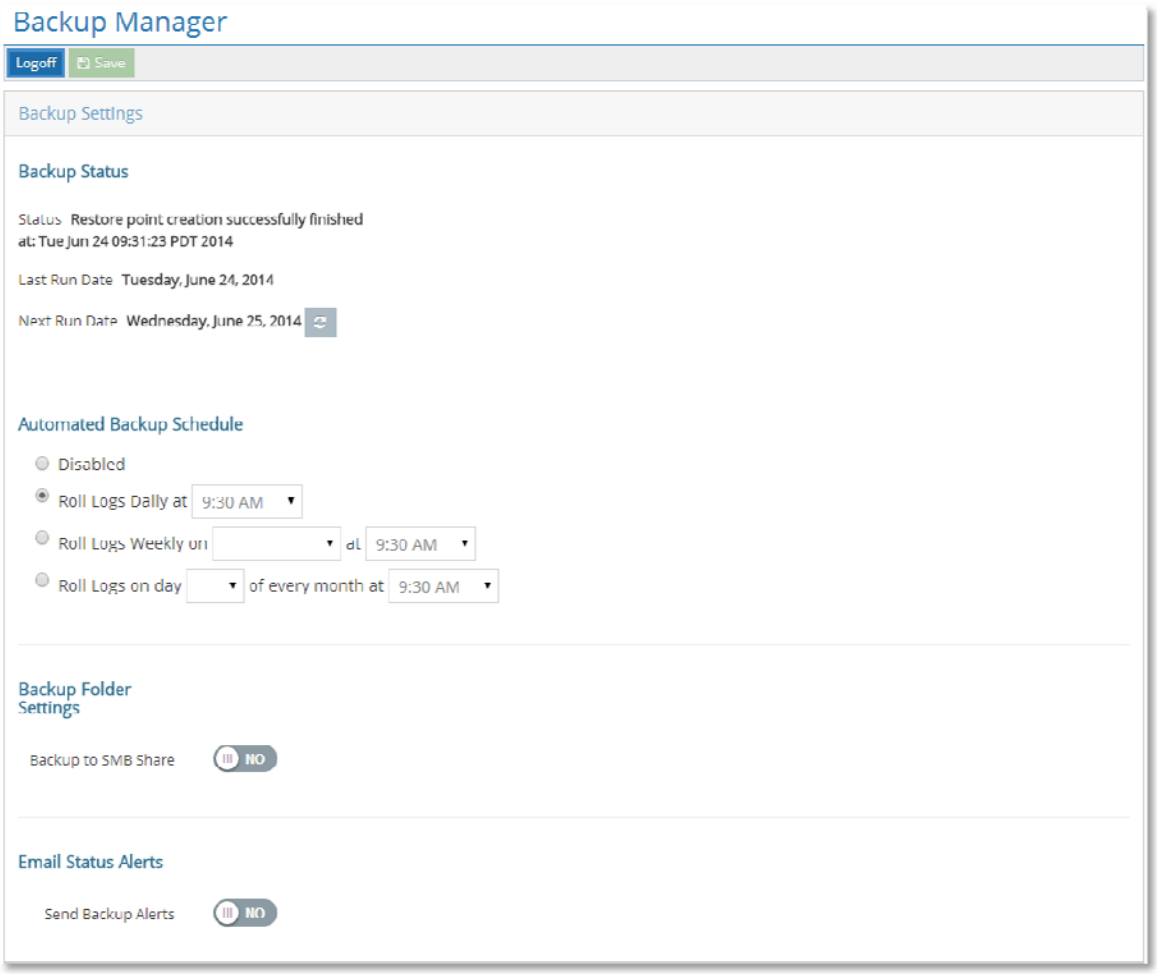


Figure 127 – Automated Scheduled Backup

You can setup a schedule to create a restore point of the settings on a daily, weekly, or monthly schedule. This saves a restore point onto the iboss device.

Backup Folder Settings – You can save these scheduled restore point backups to a SMB Share folder. You will want to enable this feature and setup the folder path and authentication settings.

Email Status Alerts – These options will allow you to use an SMTP server to email you when a backup was successfully run.